
CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2026

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Contributing Editor
Christian Schröder
Orrick



Chambers

Global Practice Guides

Data Protection & Privacy

Contributing Editor

Christian Schröder

Orrick, Herrington & Sutcliffe LLP

2026

Chambers Global Practice Guides

For more than 20 years, Chambers Global Guides have ranked lawyers and law firms across the world. Chambers now offer clients a new series of Global Practice Guides, which contain practical guidance on doing legal business in key jurisdictions. We use our knowledge of the world's best lawyers to select leading law firms in each jurisdiction to write the 'Law & Practice' sections. In addition, the 'Trends & Developments' sections analyse trends and developments in local legal markets.

Disclaimer: The information in this guide is provided for general reference only, not as specific legal advice. Views expressed by the authors are not necessarily the views of the law firms in which they practise. For specific legal advice, a lawyer should be consulted.

Content Management Director Claire Oxborrow

Content Manager Jonathan Mendelowitz

Senior Content Reviewers Sally McGonigal, Ethne Withers, Deborah Sinclair, Stephen Dinkeldein, Vivienne Button and Sean Marshall

Content Reviewers Lawrence Garrett, Marianne Page, Heather Palomino, Alison Moore, Adrian Ciechacki and Michael Irvine

Content Coordination Manager Nancy Tsang

Senior Content Coordinators Carla Cagnina and Delicia Tasinda

Content Coordinator Joanna Chivers

Head of Production Jasper John

Production Coordinator Genevieve Sibayan

Published by

Chambers and Partners

165 Fleet Street

London

EC4A 2AE

Tel +44 20 7606 8844

Fax +44 20 7831 5662

Web www.chambers.com

Copyright © 2026

Chambers and Partners

CONTENTS

INTRODUCTION

Contributed by Christian Schröder, Orrick p.6

BRAZIL

Law and Practice p.10

Contributed by Lopes Pinto, Nagasse Advogados

Trends and Developments p.26

Contributed by Bialer Falsetti Associados

CHILE

Law and Practice p.30

Contributed by Magliona Abogados

CHINA

Law and Practice p.47

Contributed by Zhong Lun Law Firm

Trends and Developments p.63

Contributed by Global Law Office

EGYPT

Law and Practice p.70

Contributed by Shehata & Partners

EU

Law and Practice p.86

Contributed by Gerrish Legal

Trends and Developments p.103

Contributed by Gerrish Legal

FRANCE

Law and Practice p.111

Contributed by Nomos

GREECE

Law and Practice p.129

Contributed by Psarras, Georgountzou - GKP Law Firm

INDIA

Trends and Developments p.149

Contributed by Shivadass & Shivadass

INDONESIA

Law and Practice p.156

Contributed by ALTA Advocates

Trends and Developments p.170

Contributed by ABNR Counsellors at Law

ISRAEL

Law and Practice p.179

Contributed by Or-Hof Law

ITALY

Law and Practice p.198

Contributed by ICT Legal Consulting

Trends and Developments p.213

Contributed by ICT Legal Consulting

JAMAICA

Law and Practice p.221

Contributed by Ramsay & Partners

Trends and Developments p.233

Contributed by Ramsay & Partners

JAPAN

Law and Practice p.237

Contributed by Mori Hamada & Matsumoto

Trends and Developments p.253

Contributed by Oh-Ebashi LPC & Partners

KUWAIT

Law and Practice p.259

Contributed by GLA & Company

MACAU SAR, CHINA

Law and Practice p.271

Contributed by Lektou – Advogados e Notários

Trends and Developments p.281

Contributed by Lektou – Advogados e Notários

MALAYSIA

Law and Practice p.285

Contributed by Christopher & Lee Ong

Trends and Developments p.302

Contributed by Christopher & Lee Ong

MEXICO

Law and Practice p.309

Contributed by Nader Hayaux & Goebel

Trends and Developments p.320

Contributed by Baker McKenzie

MOROCCO

Law and Practice p.327

Contributed by DLA Piper Casablanca

Trends and Developments p.334

Contributed by DLA Piper Casablanca

NEW ZEALAND

Law and Practice p.339

Contributed by Tompkins Wake

CONTENTS

PAKISTAN

Law and Practice p.357

Contributed by S.U.Khan Associates

QATAR

Law and Practice p.365

Contributed by GLA & Company

SAUDI ARABIA

Law and Practice p.377

Contributed by GLA & Company

SERBIA

Law and Practice p.394

Contributed by Mikijelj, Janković & Bogdanović

Trends and Developments p.404

Contributed by Mikijelj, Janković & Bogdanović

SINGAPORE

Law and Practice p.409

Contributed by Drew & Napier LLC

Trends and Developments p.426

Contributed by Drew & Napier LLC

SOUTH KOREA

Law and Practice p.432

Contributed by Kim & Chang

Trends and Developments p.446

Contributed by Lee & Ko

SWEDEN

Law and Practice p.453

Contributed by Hellström Advokatbyrå KB

Trends and Developments p.469

Contributed by Gernandt & Danielsson

TAIWAN

Law and Practice p.475

Contributed by Chen & Lin

THAILAND

Law and Practice p.491

Contributed by Chandler Mori Hamada Limited

Trends and Developments p.503

Contributed by Chandler Mori Hamada Limited

TÜRKIYE

Law and Practice p.510

Contributed by YAZICIOGLU Legal

UAE

Law and Practice p.528

Contributed by Bizilance Legal Consultants

Trends and Developments p.538

Contributed by BSA LAW

USA

Law and Practice p.543

Contributed by Chamberlain Hrdlicka

Trends and Developments p.560

Contributed by Fieldfisher

USA – CALIFORNIA

Trends and Developments p.565

Contributed by Buchalter LLP

USA – COLORADO

Trends and Developments p.570

Contributed by Buchalter LLP

USA – FLORIDA

Trends and Developments p.575

Contributed by Jones Walker LLP

USA – GEORGIA

Trends and Developments p.581

Contributed by Jones Walker LLP

USA – ILLINOIS

Trends and Developments p.588

Contributed by Seyfarth Shaw LLP

USA – MISSOURI

Trends and Developments p.595

Contributed by Sandberg, Phoenix & von Gontard, P.C.

USA – NEW YORK

Trends and Developments p.602

Contributed by Phillips Nizer LLP

USA – TENNESSEE

Trends and Developments p.607

Contributed by Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

USA – TEXAS

Trends and Developments p.614

Contributed by Buchalter LLP

CONTENTS

USA – UTAH

Trends and Developments p.620

Contributed by Kirton McConkie

USA – WASHINGTON

Trends and Developments p.627

Contributed by Miller Nash LLP

INTRODUCTION

Contributed by: Christian Schröder, Orrick

Orrick is a global law firm dedicated to serving the technology and innovation, energy and infrastructure, finance, and life sciences and healthtech sectors. With more than 1,150 lawyers across more than 26 markets worldwide, Orrick provides forward-looking, pragmatic advice on transactions, litigation and compliance matters. As one of the world's leading tech law firms, cybersecurity and privacy are central to Orrick's practice. The firm has 20 cybersecurity and privacy-focused partners and more than 60 specialised lawyers, making it one of the strongest

data protection practices in the market, recognised in the Chambers Global, US and Europe Guides. Orrick helps clients navigate the complex cybersecurity and privacy legal landscape, managing global compliance matters, cyber-incidents, litigation and regulatory investigations. The team maximises data value, addresses global privacy requirements and reduces security risks. Whether clients are managing compliance challenges, licensing data or acquiring new companies, Orrick offers forward-thinking solutions to address data challenges.

Contributing Editor



Christian Schröder is a partner in Orrick's Düsseldorf office and leads the firm's cyber, privacy and data innovation group in Europe. He specialises in data-focused laws, including cybersecurity, privacy

compliance, incident response, data licensing, AI and regulatory investigations. Christian advises on internal and external data transfers, product launches and privacy requirements for connected cars. He maintains strong relationships with German and EU data protection authorities, effectively defending clients in investigations. Recognised by Chambers as a top practitioner, he is a noted thought leader in privacy law.

Orrick, Herrington & Sutcliffe LLP

Heinrich-Heine-Allee 12
40213 Düsseldorf
Germany

Tel: +49 211 3678 7269
Email: cschroeder@orrick.com
Web: www.orrick.com



INTRODUCTION

Contributed by: Christian Schröder, Orrick

Introduction to the Data Protection & Privacy Guide

Legal and regulatory framework

As we head into 2026, data privacy continues to be an important compliance topic, a fundamental concern for individuals, businesses and governments worldwide, as digital technologies and the increasing reliance on data-driven services, such as in the context of AI, have transformed how personal data is collected, processed and shared. This has brought about significant benefits, including enhanced connectivity, personalised services and economic growth. However, it has also raised critical questions about the protection of personal data and individual privacy rights.

In many jurisdictions, data privacy laws are built on the same core principles, such as transparency, accountability and lawfulness. These principles are designed to ensure that individuals have control over their personal data and that the organisations processing this data do so responsibly. Key elements of data privacy regulation include requirements for data security and data transfers, and the rights of individuals to access, correct and delete their data.

Apart from this, a key aspect of this dynamic field of privacy protection is the constantly evolving legal landscape of data protection-related laws. The developments in 2025 brought some consolidation in Europe, acceleration in the United States and Asia, and a steady rise in complex litigation.

In the EU for instance, the AI Act and the EU Data Act (DA) moved from text to practice. In the United States, several new state privacy laws and amendments took effect on 1 January 2026, including the introduction of privacy requirements in Indiana and Kentucky. The Personal Data Protection Law (PDPL) of Vietnam came into force the same day, following its approval by the National Assembly. India's privacy law, the Digital Personal Data Protection Act (DPDPA) which finally became effective in late 2025, governs the handling of digital personal data and sets out a comprehensive framework for its collection, processing and transfer.

In many jurisdictions, existing regulations are being amended more frequently. In the EU, the draft EU

Omnibus regulation aims to simplify rules on data, AI and cybersecurity. Proposed amendments include the introduction of rules clarifying the use of personal data for AI training, a single EU entry point for incident reporting across the EU GDPR, NIS 2, DORA, and an extension of the notification time for data breaches. Meanwhile in the UK, the new Data Use and Access Act (DUAA) amends the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR). Similar developments can be observed in other jurisdictions as well, such as the amendments to Malaysia's Personal Data Protection Act (PDPA) in 2024.

Requirements for the use of and access to non-personal data

In 2025, it became clear that data-related compliance programs can no longer ignore non-personal data. In order to enable data access and sharing, jurisdictions are increasingly enacting laws to ensure that non-personal data is more accessible and usable, and that data-driven innovation is promoted.

The DA establishes new rules in the EU for how users of connected products and related services can utilise the data they generate and how data holders can derive economic value from it. In order to address the key challenges in the digital economy, the DA aims to foster a competitive data market and promote data-driven innovation, introducing premature termination rights and the right to request support when switching to similar data processing services.

With the DUAA, the UK has also started to manage non-personal data, aiming to unlock the effective use of such data. The DUAA establishes a structure for data-sharing arrangements like Open Banking (enabling third-party providers to access customer data at financial entities through application programming interfaces or APIs), which applies to both consumer and business data. This approach is comparable to the EU's DA and Data Governance Act, although the DUAA does not exactly replicate the corresponding EU regulations.

INTRODUCTION

Contributed by: Christian Schröder, Orrick

International data transfers

One of the most significant challenges in data privacy is the issue of cross-border data transfers. As data transfers are part of everyday business, regulators must address the complexities of ensuring that personal data transferred to other jurisdictions remains adequately protected. This has led to the development of various mechanisms such as standard contractual clauses (SCCs), binding corporate rules (BCRs) and adequacy decisions, which enable the international transfer of personal data in compliance with the respective data protection principles.

Many jurisdictions, particularly in the MENA region, have recently adopted this approach and published data transfer regulations that in some instances require specific approval by state authorities. For example, in 2024, Saudi Arabia published four different forms of SCCs and issued new guidelines on the use of BCRs.

In the United States, national-security-driven controls have been tightened. New federal rules constrain certain transfers of bulk sensitive US personal data to countries of concern, and the Protecting Americans' Data from Foreign Adversaries Act limits sales by data brokers to designated countries or controlled entities. These regimes sit alongside sectoral rules and state privacy laws, expanding diligence and contractual controls for global vendor chains.

China has completed the tri-path outbound data transfer framework under the Personal Information Protection Law (PIPL). Following the easing of thresholds and exemptions in 2024, 2025 saw further guidelines and, crucially, the Measures for Certification of Cross-Border Personal Information Transfers (effective since January 2026). Companies now have a choice of security assessment, standard contracts, or certification.

The UK's new DUAA establishes a new data protection standard for transfers, mandating the secretary of state to carry out a data protection test in relation to transfers of personal data to a third country or international organisation.

In the EU, international data transfers are an endless story. In 2025, the European Commission renewed

the two adequacy decisions for the United Kingdom. An adequacy decision for data transfers to Brazil is expected soon.

Due to political developments and increasing tensions with the US, doubts have been raised in Europe about the continued validity of the EU-US Data Privacy Framework (DPF) for the transfer of personal data between the EU and the US.

In September 2025, the EU General Court (EGC; Case T-553/23) dismissed an action for annulment of the DPF for the transfer of personal data between the EU and the US, thereby confirming the DPF. An appeal is pending before the European Court of Justice (CJEU).

The current situation in the EU is precarious for many companies relying on SCCs, and particularly for small and medium-sized enterprises with international ties, as an annulment of the DPF would necessitate relying on SCCs for data transfers to the US. According to the Schrems II decision of the CJEU and based on the recommendations 01/2020 of the European Data Protection Board (EDPB), the use of SCCs necessitates an assessment of the data protection level of the respective third country (a transfer impact assessment or TIA). According to the EDPB, such TIAs require a six-step review process, including a detailed examination of the legal enforcement system and surveillance laws of the recipient country. This necessitates the help of local experts and leads to increasing costs for companies, which for SMEs leads to enormous challenges.

Enforcement

In the EU, regulators continued to focus on adtech, dark patterns, the processing of sensitive data in advertising, and the processing of children's data. One particular focus of European data protection authorities has always been international data transfers. Examples are the EUR530 million fine imposed by the Irish Data Protection Commissioner against a social media platform provider for unlawful data transfers to China, and the European Data Protection Supervisor's decision to refuse a request by the European Investment Bank to transfer data to a number of non-EU/EEA countries, including Brazil, Turkey, India and Fiji.

INTRODUCTION

Contributed by: Christian Schröder, Orrick

Earlier in 2025, the EGC made a significant ruling, awarding damages for the transfer of an IP address to the United States prior to the approval of the DPF and in the absence of an adequacy decision. The court held that the website operator was liable for data transfers made through a third-party API embedded in the website, even though the transfer was not conducted by the website operator. Such decisions may have future implications for companies operating in both low-risk and high-risk contexts, as they could face mass tort litigation for using third-party services that transfer non-sensitive and device-related data to third countries.

In other jurisdictions, state privacy enforcement has also matured. In the US, the Attorneys General and the California Privacy Protection Agency pressed actions on data brokers, misconfigured consent tools, and sensitive health data in digital advertising. The development of new data localisation requirements is another important area to monitor.

Privacy litigation

Recent decisions illustrate that data privacy litigation is on the rise, with individuals and organisations increasingly seeking redress for privacy violations. In many jurisdictions, data privacy laws provide a basis for claims for immaterial damages, although the determination of such damages remains a contentious issue. Recent court decisions in the EU have clarified some aspects of compensation, emphasising that it should correspond to actual harm rather than serve as a punitive measure. However, courts tend to interpret relevant statutes broadly to ensure the efficient and continued protection of user privacy rights, which could potentially lead to more waves of mass claim litigation.

The introduction of collective redress mechanisms, such as the Representative Actions Directive in the EU, has fuelled this trend and expanded legal protection for consumers, enabling them to file collective actions for data protection violations. This current development increases liability risks for companies, particularly with cross-border implications, and highlights the importance of robust compliance programmes.

Sectoral developments

The bar is rising fast in specific sectors such as health and advertising as many regulators are increasingly focusing on these critical issues. For instance, new state health privacy laws in the US focus on purpose limitation and expectation management, demanding data minimisation and vendor oversight. With the EU Health Data Space Regulation, the EU is setting new rules for the primary and secondary use of health data and the international transfer of such data to other jurisdictions.

Enforcement remains strict, particularly regarding online marketing practices and the use of cookies. In the US, further action on deceptive design and misuse of sensitive data is expected. In France, at the end of 2025, the supervisory authority, the National Commission for Information Technology and Civil Liberties (*Commission Nationale de l'Informatique et des Libertés* or CNIL) imposed significant fines for alleged cookie violations under the French Data Protection Act, whereby a publisher was fined EUR750,000, and a financial services provider received a penalty of EUR1.5 million.

It is also notable that the DUAA is introducing changes to existing cookie regulations. Similarly, the EDPB guidelines on cookies continue to shape EU cookie laws under the ePrivacy Directive. While some jurisdictions do not have specific regulations on cookies, it is important to note that other data protection laws may still apply and set cookie requirements, particularly when cookies are related to personal data.

Conclusion

The landscape of data privacy law is complex and constantly evolving, reflecting the rapid pace of technological changes and the growing importance of data in the digital economy. The year 2026 will bring several challenges and, considering recent international developments discussed above, organisations would be well advised to start prioritising their compliance aims. They can do this by observing new incident response and reporting rules, still treating international data transfers as an evergreen risk; operationalising AI governance and expanding privacy programs to cover AI; focusing on the use and access to non-personal data (under the EU Data Act); implementing fair-terms reviews for B2B data contracts and cloud switching; and anticipating litigation and sectoral enforcement.

BRAZIL

Law and Practice

Contributed by:

Japyassú Resende Lima and Fabiana Lopes Pinto Santello

Lopes Pinto, Nagasse Advogados



Contents

1. Legal and Regulatory Framework p.12

- 1.1 Overview of Data and Privacy-Related Laws p.12
- 1.2 Rights and Obligations p.12
- 1.3 Special Categories of Personal Data p.13
- 1.4 Processing of Personal Data for Research and Development Purposes p.14
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.14
- 1.6 Data Breach Requirement p.15
- 1.7 Regulators p.15
- 1.8 Enforcement Proceedings and Fines p.16
- 1.9 Enforcement Trends p.17

2. Privacy Litigation p.17

- 2.1 Privacy Litigation Overview p.17
- 2.2 Recent Case Law p.18
- 2.3 Collective Redress Mechanisms p.18

3. Requirements for the Protection and Processing of Non-Personal Data p.19

- 3.1 Objectives and Scope of Data Regulation p.19
- 3.2 Interaction of Data Regulation and Data Protection p.19
- 3.3 Rights and Obligations Under Applicable Data Regulation p.20
- 3.4 Regulators and Enforcement p.21

4. Sectoral Topics p.21

- 4.1 Use of Cookies p.21
- 4.2 Personalised Advertising and Other Online Marketing Practices p.21
- 4.3 Employment Privacy Law p.22
- 4.4 Data Protection in M&A p.22

5. International Considerations p.23

- 5.1 Restrictions on International Data Transfers p.23
- 5.2 Government Notifications and Approvals p.24
- 5.3 Data Localisation Requirements p.24
- 5.4 Blocking Statutes p.25
- 5.5 Recent Developments p.25

Lopes Pinto, Nagasse Advogados is based in São Paulo. The firm provides expertise across many areas, including corporate and business law, tax and planning, data protection (LGPD, GDPR, and PIPL), contracts, regulation, digital assets, blockchain, transportation, logistics, labour, infrastructure, agribusiness, banking and finance, bioscience, civil law, corporate governance, compliance, tech law, and

legal risks. The team of highly skilled professionals possesses in-depth experience of national and multinational companies and law firms, and the modus operandi of organisations and businesses. Lopes Pinto, Nagasse Advogados prides itself on being a highly ethical firm, focused on achieving results and providing excellent service to its clients.

Authors



Japyassú Resende Lima is a partner at Lopes Pinto, Nagasse Advogados. He specialises in regulation, data protection (LGPD and GDPR), transportation, digital assets, blockchain, infrastructure, logistics, bioscience, agribusiness, compliance, corporate governance, and corporate law. He has a DLM (Université Bordeaux), LLM (Fordham University) and a Master's degree in Digital Business (UK) and Regulatory Law (USP/ Université de Montreal). He also has a Doctorate in Law (Université de Sorbonne) and completed postgraduate studies in business law (ESADE), economic law (Duke University) and data privacy law (LSE). He is a member of the Order of Attorneys of Brazil and the International Bar Association.



Fabiana Lopes Pinto Santello is a founding partner at Lopes Pinto, Nagasse Advogados. She has completed both a Doctorate and a Master's in Tax Law. She co-ordinates and lectures on corporate tax law at Fundação Armando Álvares Penteado (FAAP) and is also a director of communications at IASP. She is a published author in the field of tax and business law. She also speaks at national and international conferences and events on tax and other legal matters.

Lopes Pinto, Nagasse Advogados

Rua Helena, 235, 4th floor
Vila Olímpia
São Paulo
Brazil
04552-050

Tel: +55 11 2665 9200
Fax: +55 11 98311 0108
Email: contato@lopespinto.com.br
Web: www.lopespinto.com.br/



**LOPES PINTO,
NAGASSE**
advogados

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

In Brazil there are two sources of personal data protection and privacy laws: (i) primary, or original, and (ii) secondary, or derived.

Primary or original sources are concentrated in the Brazilian Federal Constitution and the General Data Protection Law (LGPD), since Brazil has adopted the centralist principle in which the protection of personal data is governed by federal rules rather than local rules. This means that any provision on the protection of personal data has its normative and conceptual origin in the Federal Constitution and the legal framework for the subject, ie, the LGPD.

Within the scope of the Federal Constitution, even before the general concept of personal data and its protection was recognised, the safeguarding of people's intimacy was already provided for in Article 5, X, considered the most essential sphere of personal autonomy. With Constitutional Amendment No 115/22, the specific protection of personal data was entered into the list of fundamental rights, becoming part of the constitutional core to be protected.

In terms of secondary or derived sources, reference should be made to the Consumer Protection Code (Law 8.078/90), which established rules for the use of personal data (it did not expressly refer to "processing") in consumer relations. Subsequently, the Access to Information Law (Law 12.527/11) was enacted. Although it did not specifically refer to personal data, it introduced rules on how citizens could exercise the right to information, provided for in the Federal Constitution (Article 5, XXXIII), reinforcing the mechanisms designed to protect the inviolability of intimacy. With the Civil Rights Framework for the Internet (Law 12.965/14), the protection of privacy was further consolidated, since the circulation of personal data and information online was afforded its own regulation.

The big revolution came in 2018, with the introduction of the General Data Protection Law (Law 13.709/18). Materially inspired by the European Union's General Data Protection Regulation, this Law gave personal

data the status of a "fundamental right protected in practice", with modern and efficient mechanisms aimed at ensuring that the processing of this data should only occur within strict and well-defined guidelines.

From then on, and particularly following the enactment of Law 13.853/19, which established the National Data Protection Authority (ANPD) and the National Council for the Protection of Personal Data and Privacy, the LGPD gained an "enforceable" arm of personal data protection, similar to the international concept of "enforcement". As a result, the ANPD, a federal agency whose main legal mandate is to regulate the processing of personal data in Brazil, began to issue key regulations on matters ranging from the role of the Data Protection Officer (DPO, referred to in the LGPD as the "Data Officer") to the international transfer of personal data.

This entire normative group, however, only has territorial scope in Brazil. The LGPD provides (Article 3, I) that its concepts and rules are applicable in so far as "the processing operation is carried out in the national territory". In other words, there is strict territoriality.

An important aspect of these rules is their relationship to legal issues regarding cybersecurity and AI. For example, the LGPD establishes that it is the obligation of the processing agent – especially the controller – to adopt cybersecurity measures (encryption, access control, cross-verification, 2FA, and others) to protect personal data.

In the field of AI, the interaction with personal data protection standards is even more significant. Suffice to mention that the mechanisms employed by AI and its developments (machine learning, active virtualisation, and others) rely on large databases to identify patterns, establish correlations, and generate results, which in general involves processing personal data, including sensitive data.

1.2 Rights and Obligations

In Brazil, the processing of personal data can only be carried out under certain principles (LGPD, Article 6):

- adequacy;

- good faith;
- purpose;
- free access;
- non-discrimination;
- necessity;
- accountability;
- prevention;
- data quality;
- accountability;
- security; and
- transparency.

Based on these principles, there are the so-called “essential requirements” for any processing of personal data. The first is that the processing must be carried out under the rules of the LGPD, which involves investigating where the data was collected, where it is processed, and for what purposes (the “triad”).

The other requirements are (Articles 7 and 11 of the LGPD):

- consent of the data subject;
- compliance with a legal or regulatory obligation by the controller;
- execution of a contract or preliminary procedures in a contract to which the data subject is a party, at their request;
- execution of public policies;
- regular exercise of rights in judicial, administrative or arbitration proceedings;
- legitimate interest of the controller or third party;
- protection of the life or physical safety of the data subject or a third party;
- credit protection;
- conducting studies by a research body; and
- protection of health by health professionals.

The LGPD also establishes the main rights of the data subject (Articles 17 and 18):

- access to personal data;
- anonymisation, blocking or deletion of unnecessary, excessive or non-compliant data;
- confirmation of processing treatment;
- data correction;
- deletion of personal data processed with consent;
- information about non-consent;

- information on shared use of data;
- intimacy;
- freedom;
- portability;
- privacy;
- revocation of consent; and
- ownership.

In the context of the processing of personal data, meeting the principles and respecting the rights is not sufficient. Each processing agent – controller and operator – must observe the “organic requirements” for this processing. The main “organic requirement” is the centralised and unitised control of personal data processing operations, provided for in Article 37 of the LGPD. This requires that the agent should institute, maintain, and manage a system capable of providing, in real time, up-to-date information on the circularity of personal data in the organisation, including the categories of data, the purpose of the processing, and the protection measures in place.

In this sense, the processing agent should consider adopting strict and transparent internal policies, protocols for the regular processing of data, specific procedures and, at a more objective level, control tools, such as the assessment of the impact of the processing on the privacy of individuals and the assessment of legitimate interest (LIA).

1.3 Special Categories of Personal Data

Sensitive data, which the LGPD defines as that referring to racial or ethnic origin, religious conviction, political opinion, union membership or religious, philosophical or political organisation, health, sex life, genetics or biometrics (Article 5, II), receive special protection under the law.

In this sense, this data may (or should only) be processed under the following bases:

- consent;
- compliance with a legal or regulatory obligation by the controller;
- execution of public policies;
- regular exercise of rights in judicial, administrative or arbitration proceedings;

- guarantee of fraud prevention and the security of the data subject;
- protection of the life or physical safety of the data subject or a third party;
- conducting studies by a research body; and
- protection of health by health professionals.

Personal data related to children and adolescents may also be processed, but the legislation requires that this be done under an unclear criterion of the “best interest”. This means that processing this type of personal data must consider the special protection given to the intimacy and privacy of children and adolescents, without creating an insurmountable restriction. The legislation also imposes two conditions: the processing must comply with the principles and rules of the LGPD and, in the case of children, the consent of a parent or legal guardian is required.

1.4 Processing of Personal Data for Research and Development Purposes

In the context of the processing of personal data for research and development, especially of health and life protection products and services, the subject is more complex and must be evaluated from two angles: that of the processing carried out by the government and that of the processing resulting from applications and mechanisms provided by private companies.

The LGPD provides (Article 13) that it must occur within the public entity – which, in other words, means that hiring third parties for processing and sharing the data is not allowed – and under strict security and reliability protocols, including anonymisation or pseudonymisation.

Even in these cases, the processing must respect the principles and requirements of the LGPD, especially if it involves handling of sensitive data or data of high relevance to individuals.

The same level of care applies to the processing resulting from applications and mechanisms provided by private companies (MedTechs, HealthTechs, etc).

Even stricter criteria may also apply. For example, in the case of R&D, the processing of personal data must be based on a “strictly legitimate purpose”, ie, one

that, in origin, has a legitimacy that cannot be questioned. In addition, the processing must be based on irreversible anonymisation, in which the data cannot be linked to a specific person and which, therefore placing it outside the rules of the LGPD.

In terms of commercial use of this data, Brazil follows the European system: it is prohibited to process the data for commercial purposes or to achieve economic advantage, except for the provision of health services.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

In the context of personal data processing and AI, two premises are strictly essential: “human in the loop” (“human on the top”) and strict compliance with data protection legislation.

These principles give rise to some requirements. The first is that the use of personal data in AI systems, models, or resources must always consider risk-based regulation, which prohibits AI being used for behavioural manipulation or sensitive categorisation (eg, the use of biometric data). The second is the strict and rigorous assessment of high-risk AI, considered to be systems that can significantly impact fundamental rights, public safety or the health of the population, in line with the criteria of the European AI Act. The third requirement is that AI should always be subject to active human supervision, especially in the case of automated decisions.

In Brazil, the regulation of AI is still under discussion. The most recent document in this regard is Bill 2,338, approved by the Senate and currently under consideration in the Chamber of Deputies. According to the Bill, some high-risk categories should require much stricter restrictions, such as employee recruitment and selection, justice and law enforcement, and facial recognition and biometrics.

The Bill also considers some modalities of AI as excessive risk (Article 14), and as a result prohibits models whose objective is, for example, behavioural manipulation, real-time biometric identification, and emotion recognition.

1.6 Data Breach Requirement

The expression “data breach” is part of a larger category of events harmful to personal data called “security incident.” Resolution CD/ANPD 15/24 defines a security incident as “any confirmed adverse event, related to the violation of the properties of confidentiality, integrity, availability, and authenticity of personal data security” (Article 3, XII).

In general, a security incident can encompass different types of attacks on personal data, including the violation itself, improper disclosure, and data leakage, ranging in severity from the most minor to the most serious.

The Brazilian regulator has established a set of measures necessary to deal with a security incident, manage its effects and prevent its repetition over time, as outlined below.

- Communication to the regulator: the controller must formally notify the ANPD of the incident within three days of the occurrence.
- Communication to the data subject: the controller must formally communicate the incident to the data subject within three days of becoming aware that the incident has affected the data subject’s data.
- Information: the controller must include, in the communication, a description of the nature and category of personal data affected.
- Recordkeeping: the controller must maintain a detailed record of the incident for five years.
- Management: the DPO takes over the management of the incident.
- Compliance: the controller and DPO establish how and to what extent regulatory compliance was impacted by the incident.

A security incident may require an inspection action by the regulator, with or without the application of penalties. However, there is always the possibility that an incident that compromises a large amount of data or exceeds the controller’s limits will be investigated by the ANPD or even by the Public Prosecutor’s Office. In addition, an incident may also lead to claims for indemnification (reparation) against the controller,

requiring it to compensate data subjects for losses and damages (LGPD, Article 42).

1.7 Regulators

In Brazil, the regulatory authority for personal data and its protection has been well established since Law 13,853/19, which created the ANPD.

This authority is competent to, among other responsibilities (LGPD, Article 55-J):

- co-ordinate with public regulatory authorities to exercise their powers in specific sectors of economic and governmental activities subject to regulation;
- enter into an agreement with processing agents to eliminate irregularities, legal uncertainty or litigation in the context of administrative proceedings;
- deliberate, in the administrative sphere, on a conclusive basis, on the interpretation of this Law;
- provide for the forms of publicity of personal data processing operations;
- issue regulations and procedures on personal data protection and privacy, as well as on personal data protection impact reports for cases in which the processing represents a high risk to the guarantee of the general principles of personal data protection provided for in this Law;
- draft guidelines for the National Policy for the Protection of Personal Data and Privacy;
- supervise and apply sanctions in the case of non-compliant data processing, through an administrative process that ensures the adversarial process, full defence and the right to appeal;
- implement simplified mechanisms, including by electronic means, for the registration of complaints about the violation of this Law; and
- promote co-operation with personal data protection authorities in other countries, of an international or transnational nature.

The ANPD’s role, although predominantly guiding (at this stage of Brazilian legislation), has a strongly instructive, supervisory and sanctioning character.

This is possibly why its investigative process, especially regarding direct violations of personal data protection legislation, is especially detailed. Under the

General Coordination of Inspection (CGF), the focus of this process is to evaluate, analyse and determine the level of compliance with the General Data Protection Law by processing agents, and may have a preventive or repressive nature.

The sequence is:

- the investigation can start with reports from data subjects, notifications of security incidents, impact reports or sample inspections;
- the ANPD notifies the processing agent to present information, evidence, and proof, which may include document collection and even local audits;
- the ANPD verifies the consistency of the responses, and some measures, especially prevention, can be adopted at this stage;
- opening of an Administrative Sanctioning Proceeding (PAS), if the irregularities continue or are sufficiently serious;
- establishment of the PAS and notification of the investigated party;
- production of evidence and analysis of facts by the technical area of the ANPD;
- the processing agent can present their defence;
- decision on the application of sanctions, with the possibility of appeal; and
- deadline for the investigated party to appeal.

The issue of binding status still generates debate, but in general it is understood that the ANPD's decisions are binding, albeit in a stricter sense. This means that they bind personal data processing agents (controllers and operators) and are definitive in the administrative sphere, after the applicable appeals. However, the “atypical” binding, the one referred to other spheres of power or to agents who did not participate in the administrative process, remains debatable. This is the case, for example, for ANPD investigations shared with the Administrative Council for Economic Defense (CADE), whose use could inform the internal proceedings of this Council on anti-competitive practices. Although such co-ordination exists, the binding effect, due to the lack of essential legal prerequisites, is not yet fully mandatory in these cases.

1.8 Enforcement Proceedings and Fines

Investigative actions within the scope of the ANPD begin with the General Coordination of Inspection (CGF), and from there unfold within a very specific procedure.

A complaint, a news item or an event of public knowledge can start an investigation. At this stage, the ANPD is presented with a “cold fact”, raw material for analysis. The next stage is the preparatory procedure, which, even though it is not mandatory, allows the ANPD to collect preliminary elements to support a potential PAS. The next step is the collection of evidence by the Regulator's technical team, which searches different sources for the material necessary to “instruct” the investigation process. Subsequently, the party being investigated, who may be a personal data processing agent, is notified and has ten business days to respond.

According to the LGPD, different penalties can be applied to cases of violation of legal rules on personal data. The sanctions list (LGPD, Article 52) includes:

- warning;
- fines of up to 2% of the revenue of the private legal entity, group or conglomerate, limited, in total, to BRL50 million per infraction;
- daily fines, subject to a total limit (see previous bullet);
- publication of the infraction;
- blocking of the personal data to which the infraction refers until it is regularised;
- deletion of the personal data to which the infringement refers;
- partial suspension of the operation of the database to which the infraction refers;
- suspension of the exercise of the personal data processing activity to which the infringement refers; and
- partial or total prohibition of the exercise of activities related to data processing.

As for the criteria for setting penalties, the legislation provides that the seriousness and nature of the infraction, the size of the offending agent, the advantage obtained or intended, recidivism, the co-operation of the agent, the mitigation measures adopted by

them and their economic situation may be taken into account.

1.9 Enforcement Trends

There have been many developments in recent months in terms of privacy, security in the processing of personal data and inspection, especially in the expansion of certain basic concepts.

Some notable events include the following.

- The advancement of operations with crypto-assets has required that extra care be taken with personal data, especially those submitted to blockchain-based trading. These operations often involve personal data of the traders that crosses borders, which implies international sharing and indistinct storage.
- The pressure on the processing of sensitive personal data has significantly increased. The LGPD's protection of this data does not seem to be sufficient to stop practices such as "biotyping", passive biometrics, and the transfer of databases without the knowledge (and even without agreement) of the data subjects.
- The judiciary has explicitly recognised, following a decision of the Superior Court of Justice (STJ), that there is presumed moral damage (without the need for explicit proof) if a processing agent shares personal data without the knowledge or agreement of the data subject.
- The international transfer of personal data has gained more attention from the ANPD, following the publication of Resolution 19, which imposes stricter conditions on this transfer.

For organisations, there are many lessons:

- policies are insufficient; it is necessary to demonstrate the complete mapping of data flows (dynamic), so that the data subject knows how and for what purpose their data is processed;
- embed privacy considerations from the outset when developing new AI products, services, and algorithms;
- implement quick and effective incident response plans;
- liability for personal data is joint and several;

- adopt rigorous anonymisation and pseudonymisation techniques when dealing with sensitive data and train AI models to minimise risk.

Privacy is now treated as a competitive differentiator and a driver of customer loyalty (privacy-led marketing), beyond just a compliance requirement.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Arguably, the number of litigations and disputes involving privacy and personal data is growing year by year. These conflicts are no longer about financial issues, but relate to the improper, unauthorised, rights-violating or even illegal use of personal data for commercial purposes, and in some cases, illicit activities.

With the consolidation of the LGPD and the structuring of the ANPD, the trend towards greater judicialisation is being observed at different levels, including in the main Brazilian courts.

Litigation has originated from these main sources:

- security incidents;
- misuse of personal data;
- inadequate processing, without purpose and without legal basis;
- invasive biometrics;
- sharing for financial purposes;
- violation of minimum rights by some mass consumer companies;
- improper commercial profiling; and
- use of personal data to contract unsolicited services.

These disputes range from personal data subjects and consumers to civil society entities and the Public Prosecutor's Office. There are already signs that groups of data subjects, impacted by the misuse of their data, are organising to file complaints with the regulator, establishing a regulatory basis for relevant lawsuits. Employees, with the support of their unions, are taking action against practices such as the use of biometric data by companies to monitor working

hours in remote work and the so-called “broad base”, a non-formal platform that gathers personal data of various types, including sensitive data, to establish behavioural patterns and guide hiring decisions based on employee profiles.

Litigation related to personal data and privacy has also strongly influenced the courts, which now recognise convictions based on presumed moral damage, or even moral damage for the repeated practice of violations of personal data legislation. Although with some caution, jurisprudence already considers that, under certain circumstances, moral damage arises from the mere absence or ineffectiveness of internal mechanisms of organisations, which results in security incidents. Incidents which were previously considered “external fortuitous” (attributable to causes beyond the control) are beginning to be seen as an “internal failure”, a defect in practices and policies, under the responsibility of the personal data controller.

Assessing the effects of a data breach, for example, is still done cautiously, and on a case-by-case basis. Factors include if the violated data is sensitive, if the impacted person is a child or elderly, if the event had public repercussions, or if it was nothing more than a mere inconvenience.

2.2 Recent Case Law

More recently, some courts, especially the one in São Paulo, have decided that “hacker” attacks on systems cannot always be considered an “external fortuitous” (cause beyond the control of the organisation). If the company does not demonstrate, with evidence, that it adopts and practices adequate security measures, the case is one of “internal fortuitousness”, in line with the principle of accountability (LGPD, Article 6, X).

Another important basis for decisions is to consider that the data controller is only exempt from being liable for a personal data breach if it proves one of the so-called “exclusions”, as provided for in Article 43 of the LGPD.

At the end of 2025, the Superior Court of Justice recognised the existence of presumed moral damage in a case of sharing personal data related to the monthly income, address, and personal telephone numbers

of consumers to third parties, regardless of proof of actual harm, on the grounds that this type of conduct violates the legitimate expectations, privacy, and personality rights of the data subject.

2.3 Collective Redress Mechanisms

A topic under discussion in Brazil is whether there is a basis for collective or diffuse (indistinct) compensation for damages resulting from violations of personal data protection legislation.

In general terms, collective redress in Brazil is a regulated and mature matter in the courts, serving to safeguard rights that are not strictly individual and to provide financial compensation (if applicable), based on the Federal Constitution and developments under the Consumer Protection Code and the Public Civil Action Law (Law 7.347/85).

What has been put to the test is whether, in the context of personal data as a fundamental right, in which the privacy and intimacy of individuals are at stake, collective or diffuse remedies are the most appropriate.

The General Data Protection Law does not refer to “diffuse damage”, but to “collective damage” (Article 42). The distinction matters. In cases of “diffuse damage”, the impact falls on an indistinct set of individuals, not necessarily belonging to a specific or determined collective. In the case of “collective damage”, a group or class of individuals is impacted, directly or indirectly, and thereby acquires the right to seek reparation. Therefore, if a security incident impacts not only certain individuals, but a collective of them, the legal framework for comprehensive reparation (“collective”) applies. This reparation covers both the patrimonial (material) and the moral (immaterial) aspects, and the controller or operator is fully responsible.

Collective damage can be claimed by the Public Prosecutor’s Office, the Public Defender’s Office, the Union, states, municipalities or legally constituted associations.

However, the reparability of the damage requires the fulfilment of certain conditions. First, the damage must have resulted from the activity of the processing agent

with respect to the personal data under their control, that is, data that they themselves handle. Second, the responsibility of the processing agent must be evidenced, not assumed. In this regard, one of the most important discussions is whether this liability is objective or subjective, that is, whether it depends on a conscious or assumed attitude of the agent (recent court decisions indicate that this liability is objective). Third, the harmful event must be assessed against the exclusions provided for in the LGPD (Article 43), which can relieve the processing agent of the responsibility for the event and, consequently, the obligation to provide compensation or reparation.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

In Brazil, the regulation of the internet of things (IoT) has advanced significantly, but there are still no specific provisions on the protection and processing of non-personal data in this field.

However, some non-specific laws deal with this subject.

- Industrial Property Law (Law 9.279/96): deals with the protection and processing of non-personal data in the context of business secrets and confidential technical elements.
- Civil Rights Framework for the Internet (Law 12,965/14): establishes principles, guarantees, rights and duties for the use of the internet, including keeping records of connection and access to applications in general.
- Sectoral regulations: agencies such as the telecommunications regulator (Anatel) and the Central Bank (Open Finance) have guidelines on the sharing of non-personal data in financial services.

In general terms, companies also use some non-personal data protection mechanisms within the scope of their respective businesses:

- non-personal data processing agreements;
- cloud and IoT contracts; and
- non-personal data protocols.

However, one issue worries companies and regulators: the so-called “gray area”, or “inflection zone”. This arises when certain activities involve the coexistence of the processing of personal data with the processing of non-personal data. In such cases, due to the existence of “associated personal data”, the LGPD applies, at least in a dominant or preponderant character.

Brazil does not yet have its own Data Act, such as the EU Data Act, which determines who can access and make use of data generated by connected products (the “provenance data”). The ANPD has intensified studies on anonymisation and may, in the coming months, regulate the use and sharing of IoT technical data.

Something that can help a lot in this regard is that Brazil and the European Union have now mutually recognised (in the case of the EU this happened very recently, in 2026) that their respective personal data protection systems offer an adequate level of protection for this data. This is a significant development, which may even facilitate the procedures for the international transfer of personal data between the two blocs.

3.2 Interaction of Data Regulation and Data Protection

The interaction between data protection and data protection adopts, in general terms, the integrative principle. This means that the two subsystems (legislative and regulatory) are harmoniously co-ordinated to offer individuals a set of safeguards that work with each other. In this way, while the legislation (especially the LGPD) places the processing of personal data within specific guidelines (requirement for legal bases, observance of principles, greater care with sensitive data, etc), regulation operates at a higher level, seeking to order and discipline the behaviour of processing agents and ensure compliance with the legislation, including sanctions.

If the LGPD establishes that the processing of personal data is only possible within the established legal hypotheses (the so-called “legal bases” in Articles 7 and 11) and that non-compliance may generate penalties and an obligation to repair damages, the regula-

tion (through the ANPD and its rules) works to ensure that these legal requirements are met from a “macro” point of view. The government can use mechanisms (inspections, audits, etc) to ensure that the guidelines established by the LGPD are observed.

On the other hand, there is the relationship between this framework and non-personal data. In general terms, if there is personal data being processed, whether alone or in combination with non-personal data, or even with strictly technical data (which does not touch on aspects of privacy and intimacy of individuals), the LGPD applies and also applies to the regulatory data exercised by the ANPD. This concept, known as “cross-regulation”, allows different regulators to act within the same process, each in its own scope of action, so enabling “extended protection” to occur.

In this sense, the different regulators interact to ensure, for example, “privacy by design” and “privacy by default.” This means, for example, that AI systems and capabilities must be created and configured to also protect data automatically, that personal data in model training must be protected by measures (such as anonymisation) to prevent the AI model from “decorating” and exposing sensitive data (data inversion), and that privacy impact assessments (DPIA) are made on high-risk AI systems.

3.3 Rights and Obligations Under Applicable Data Regulation

The idea of “regulatory interaction” (which Brazil has adopted, at least in part), although useful and operational, reflects a distinction also adopted by the EU Data Act: personal data, which directly relate to the privacy and intimacy of individuals, and non-personal data, which focus on competition, innovation, access, sharing, and invention. In both cases, organisations move away from the role of “owners” of data and assume that of “controllers”; this change has strong legal and legal impacts.

In the context of strictly personal data (typically personal, related to the privacy and intimacy of individuals), the focus is on its protection, since this has to do with fundamental rights, established by the Federal Constitution. “Protection” includes a whole set of legal and regulatory guidelines, such as:

- access (LGPD, Article 9);
- confirmation of existence (LGPD, Article 19);
- portability (LGPD, Article 18, V); and
- revocation of consent (LGPD, Article 18, IX).

In the field of non-personal data (not related to natural persons), the idea of “protection” is mainly related to the following.

- Sharing: this should only occur under “FRAND (fair, reasonable and non-discriminatory)” conditions, which can help prevent holders of essential patents from refusing to license them or demanding abusive fees, impacting competition and technological innovation.
- Right of access and use: users (companies or consumers) have the right to access data generated by connected products and services, most often in real time.
- Interoperability: users have the right to replace data service providers or providers, including cloud switching.
- Protection of secrets: manufacturers and developers can refuse to share data if there is a risk of exposing industrial secrets.
- Termination with migration: users must be guaranteed data portability at the end of their contract, without facing abusive fees.

For both personal and non-personal data, organisations must take certain actions, including:

- update storage, update and deletion policies, to ensure that at the end of the contractual relationship portability is possible, with rollback and contingency plans;
- implement standards for data portability between cloud providers with a reduction (or elimination) of switching fees;
- implement safeguards that are at least reasonable against unlawful access to data by third governments;
- include FRAND terms in non-personal data contracts;
- map data generated by IoT devices and ensure that the interface allows direct user access to the data;
- react in terms of infrastructure;

- review policies and agreements on personal data; and
- review contracts and data agreements in general.

3.4 Regulators and Enforcement

For personal data, the Brazilian authority is the ANPD, as established in the LGPD, Article 55-J, I.

A recent issue involves the ANPD's competence to "ensure the observance of commercial and industrial secrets" (LGPD, Article 55-J, II, and ANPD Ordinance 1/21, Article 16, XXI). Commercial and industrial secrets, in general, fall within the Industrial Property Law (Law 9.279/96), which provides penalties for acts of violation of these secrets, since secrecy is essential to safeguard the competitiveness and economic value of the information. In practice, what the LGPD establishes (or should be understood to establish) is that the protection of personal data must also account for the protection of commercial and industrial secrets related or linked to them. This means that the ANPD does not technically have "direct" authority over these secrets, but a derivative or ancillary role in ensuring their protection.

For non-personal data, other Brazilian regulatory entities can act, such as CADE, in the case of competition issues (or linked competition), Anvisa, ANS and even, for financial services and products, the Central Bank.

4. Sectoral Topics

4.1 Use of Cookies

Online tracking (and its derivatives, such as active tracking) and its technologies, including the use of cookies, web beacons, fingerprints, and SDKs (Software Development Kits), are governed by the Brazilian LGPD. In practice, this method of obtaining a person's location in real time suggests that data from individuals can be accessed and used both to distinguish them from others and to know where they are, eliminating other possible places. As a result, regulation falls on the ANPD.

The fundamental requirement for compliance in these cases is that the collection of personal data is transparent and based, whenever possible, on the user's

consent, allowing the user to manage their own settings.

For consent models, it is possible to apply the following approaches.

- Opt-in: requires prior, free, informed and unambiguous consent for the use of cookies that are not strictly necessary, such as tracking cookies for personalised advertising or behaviour analysis.
- Opt-out: for strictly necessary cookies (technical or functional), which guarantee the proper functioning of the page in navigation.
- Third-party and tracking cookies: pure opt-out (first track and then give the option to opt-out) is not recommended as the best compliance by the ANPD.

In any scenario, certain "essential rules" must be applied, as follows.

- Third-party cookies: being more invasive, they require greater rigour in obtaining consent, as they track the user on different pages and applications.
- Children and adolescents: require extra safeguards, via measures proportional to the risks.
- Preference management: a cookie banner must be adopted for the user to reject or accept specific categories of cookies.
- Transparency: pages and applications must have a "Cookie Policy", explaining what personal data is collected, the purpose and the duration of storage.

4.2 Personalised Advertising and Other Online Marketing Practices

In the national territory, personalised and targeted advertising in Brazil is basically regulated by the LGPD, the Consumer Protection Code and, at some level, the Brazilian Code of Advertising Self-Regulation (CONAR).

This type of activity depends on some conditions, including:

- free, informed, specific and unambiguous consent (if used), preferably with an active confirmation (opt-in), via pre-checked boxes;

- the ECA Digital (Law 15,211/25) has specific rules for digital platforms, prohibiting the profiling of children and adolescents for targeted advertising, including the requirement of age verification mechanisms and parental consent;
- explicit purpose and well-established legal basis (LGPD, Articles 7 and 11);
- non-discrimination and non-abusiveness (undue intrusion);
- children's advertising is considered an abusive practice, according to the CDC (and CONAR's understanding), due to the vulnerability and inexperience of the target audience;
- content restrictions for certain audiences (children and the elderly, for example, via sectoral agreements or good practices in advertising and content marketing); and
- transparency for the data subject.

4.3 Employment Privacy Law

In the context of work and related activities, even outside the company's physical environment, compliance depends on the application of the LGPD and the Consolidation of Labour Laws (CLT). This is a typical case of combined regulation, in which two systems come together to protect the privacy and intimacy of workers. In a way, this harmonises the employer's directive authority (CLT, Article 2), the employee's self-determination and fundamental rights, including the protection and control of their personal data.

The monitoring of employees (considered work monitoring) is permitted under the legislation and by the courts, but without exaggeration, with reasonable prudence and with specific criteria, including:

- background checks: only in exceptional situations, where the nature of the function or the level of trust requires it;
- BYOD (Bring Your Own Device);
- control of working hours: monitoring must respect private life;
- candidate data: collect only those strictly necessary for the vacancy;
- specific and explicit purpose: monitoring must not be generic;
- limited to the professional context: monitoring must not extend to personal or family matters;

- work tools: monitoring can include professional tools; and
- transparency.

4.4 Data Protection in M&A

In an M&A scenario, attention to personal data and to the privacy and intimacy of individuals must be rigorous and absolute. The risks increase, and the possibility of a security incident increases as negotiations progress. In addition, commercial and industrial secrets, in general associated with individual developers and inventors, whose data may be in evidence, are at stake.

In this context, some requirements are non-negotiable, including the following.

- Legal basis: avoid diffuse bases, including for sharing.
- Purpose of the processing of personal data: must be precise, objective, explicit (non-generic) and transparent.
- Mapping and stratification of risks in the target (company).

In due diligence, the following practices should be observed.

- Cautious sharing: minimised the exchange of documents with personal data.
- Use of anonymised or aggregated information whenever possible.
- Secure virtual data room (VDR): data transfers must take place in secure digital environments, with access control, encryption, and audit logs.
- Confidentiality agreements (NDAs) must include data protection clauses, holding the parties responsible for their improper handling.

On the change of control and signing, the following applies.

- R&W (representations and warranties): purchase and sale agreements (SPAs) must have representations and warranties confirming that the target company follows the LGPD.
- Risks and indemnities: due diligence can reveal data liabilities, which leads to adjustments in the

purchase price or specific indemnification clauses for regulatory sanctions.

- **Transfer of assets:** in the transfer of databases, it must be verified that the original purpose of the collection of personal data allows the transfer to the new controller and that it does not constitute an international transfer of personal data.

For the internal transparency notices, the following applies.

- **Data subjects** (customers, employees and others) must be notified of the change of controller (especially if there is a change in the way their data will be processed).
- **Opt-out and consent** (or authorisation): it may be necessary to notify the data subjects and allow them to exercise their rights, including opt-out if the future processing is incompatible with the original purpose.

For post-closing considerations, the following should be observed.

- **Deletion of unnecessary data:** data not necessary for business continuity must be deleted or anonymised.
- **Systems audit (legacy):** legacy systems of the acquired company may be vulnerable. Technical integration must ensure that the security of personal data is maintained (security by design).
- **Policy harmonisation:** unify privacy policies of the buyer and the acquiree.

5. International Considerations

5.1 Restrictions on International Data Transfers

The topic of international transfer of personal data has been under discussion in Brazil since the entry of the General Data Protection Law in 2018. Considered as “external sharing”, international transfer brings many serious challenges, such as the risk of “infinite dispersion” of data and the difficulty of its repatriation when the processing ends or can no longer be carried out.

Recently, the ANPD issued Resolution 19, which specifically addresses this issue. According to the Resolution, transfer is the “processing operation through which a processing agent transmits, shares or makes available access to personal data to another processing agent”. If the agent receiving the data is outside Brazil, the transfer is international, as established by the LGPD (Article 5, XV), which considers it as a movement “of personal data to a foreign country or international organization of which the country is a member”.

In the LGPD, the international transfer of personal data is permitted (Article 33), but only:

- to countries or international organisations that provide a level of protection of personal data adequate to that provided for in this Law;
- where the national authority authorises the transfer;
- where the transfer is necessary for international legal co-operation between public intelligence, investigative and prosecution bodies, in accordance with the instruments of international law;
- where the transfer is necessary for the execution of public policy or legal attribution of the public service, with prior public disclosure in accordance with Article 23, I of this Law;
- where the transfer is necessary for the protection of the life or physical safety of the data subject or a third party;
- where the transfer results in a commitment assumed in an international co-operation agreement;
- where necessary to comply with items II, V and VI of Article 7 of the LGPD;
- where the controller provides guarantees of compliance with the principles, the rights of the data subject and the data protection regime provided for in the LGPD, in the form of:
 - (a) specific contractual clauses for a given transfer;
 - (b) standard contractual clauses;
 - (c) global corporate standards;
 - (d) regularly issued seals, certificates and codes of conduct; and
- where the data subject has provided their specific and informed consent to the transfer.

In the above-mentioned Resolution 19, the ANPD also established which standard clauses must be adopted by controllers if the international transfer of personal data can use this mechanism.

Fortunately, with regard to the European Union, the EU and Brazil already recognise that both personal data protection systems (GDPR and LGPD) are equivalent, which facilitates international transfers based on “essential equivalence” (LGPD, Article 33, I).

5.2 Government Notifications and Approvals

For the international transfer of personal data, some protocols and conditions must be met, especially after ANPD Resolution 19.

An international transfer of personal data can only occur under one of the “specific regulatory conditions” established by the LGPD (Article 33). In practice, each of these “regulatory conditions” is an “additional legal basis” (in addition to those provided for in Articles 7 and 11 of the LGPD) for the transfer, a kind of double layer of protection. This allows the data subject to be sure that their data will only be shared with another nation under the legal guarantee of “formal and material adequacy”, the so-called principle of double command.

In international transfers of personal data, some guarantees are required, such as:

- although regulatory approval is not required for each transfer, the use of at least one of the mechanisms provided for in Article 33 of the LGPD is mandatory;
- express purpose and well-established legal basis;
- data mapping, security assessment, and implementation of safeguards;
- it may also be necessary to base the transfer on Binding Corporate Rules (BCRs) if the transfer takes place within the same economic group, provided that they are approved by the competent data protection authority; and
- an impact assessment (TIA) may be required – the national controller must assess whether the legislation of the destination country compromises data protections.

For international transfers of non-personal data (any data not directly related to the privacy of individuals) certain safeguards are also required, including:

- express purpose and transparent purpose;
- some European and US standards (such as ITAR or EAR) require approval to transfer technical data, software, or technology to “unauthorised persons” or embargoed countries;
- formal request to government agencies;
- compliance with bilateral or multilateral treaties;
- identification of a compliance officer;
- knowing precisely what data is going out and who will receive it;
- contracts with standard clauses or evidence of encryption; and
- legal assessment, ie, making sure that the transfer does not violate security or privacy laws.

5.3 Data Localisation Requirements

Neither the LGPD nor the Brazilian data regulator clearly imposes a restriction on the location of personal data, which means that, by definition, the data does not need to be stored exclusively in Brazil, or even physically located in Brazil. In practice, the data must be “locatable”, but not necessarily “localised”, that is, processing agents must know where the data can be found, but this does not necessarily imply that it must be stored in a specific country or confined to a specific storage location.

However, some sectors, such as finance, have more explicit rules on the location of personal data. The Central Bank, for example, as a regulator, requires that financial institutions that use cloud services hosted abroad must ensure full and immediate access to data by the Brazilian regulator. If the cloud is in a country without a co-operation agreement with the Central Bank, the contracting requires prior authorisation from this regulator (CMN Resolution 4,893/21, Articles 11 and 12). The health sector is another that sets limitations on the international transfer of data related to clinical research, the development of medical resources and pharmacology. In particular, raw, sensitive and restricted data must be kept locally or transferred under confidentiality rules.

Remote access is another hot topic. As a rule, remote access is considered an international transfer of data, especially personal data. Under the LGPD, access (which is a form of processing, Article 5, X) does not require data and those who access it to be in the same country. It follows that access from Brazil to personal data in another country does constitute an international transfer and is therefore subject to the requirements of the LGPD and Resolution No 19 of the ANPD.

5.4 Blocking Statutes

Blocking statutes are basically legal norms adopted by a country or economic bloc to prevent or nullify the effects of the legislation of other countries that try to impose sanctions or trade restrictions, which can protect local companies or economic sectors from foreign penalties or sanctions.

There are different mechanisms for the recognition of foreign court decisions and data protection laws (especially governing personal data) that greatly restrict foreign discovery, compliance with sanctions, and the cross-border transfer of personal and non-personal data. In practice, it is a safeguard based on the principle of extraterritoriality, whose main mission is to protect national sovereignty, commercial and industrial secrets and the privacy of citizens.

Some countries, such as Canada, China, and France, have passed laws prohibiting citizens and companies from providing documents or information to foreign court proceedings unless under international treaties such as the Hague Convention on the Taking of Evidence Abroad. In Brazil, the Federal Supreme Court continuously reaffirms that foreign laws and acts do not have automatic legal effects in Brazil, since they depend on a local homologation process or, at least, on international co-operative acts.

The blocking rules, even if they were not created with personal data in mind, act as a “formal reinforcement” of the legislation for the protection of this data. A good example of this is the LGPD, which prohibits the international transfer of personal data to countries

that do not guarantee an adequate level of protection similar to that of Brazil. In this sense, the discovery (the production of evidence) that involves or depends on personal data, without valid authorisation, violates the LGPD.

5.5 Recent Developments

In terms of the international transfer of personal data, the most recent development, which is highlighted in Brazil and the European Union, is that both parties have recognised that their frameworks for the protection and safeguarding of personal data are “materially equivalent” and ensure an adequate level of protection (decision of the European Parliament of 1/26/26 and ANPD Resolution 32).

Another development refers to the EU-US Data Privacy Framework (DPF), whose validity was upheld in September 2025 by the General Court of the European Union, which reinforces legal certainty for EU-US transfers.

Other developments are also underway, for example:

- the transfer of non-personal data to more advanced research countries;
- “relativised” international transfer where the data is “dual-localised”, stored in the country of origin and in a destination country; and
- transfer for an essential period.

In addition, changes are expected in the near future:

- intensification of regulatory oversight of the ANPD;
- more requirements for personal data mapping and privacy impact reports;
- stricter obligations for personal data policies;
- ANPD must publish a list of countries considered safe for data transfers (adequacy decisions);
- the DPF may face new legal challenges through activists, despite its retention;
- focus on sensitive data and AI; and
- emergence of new concepts such as “reserved data” and “data in process”.

Trends and Developments

Contributed by:

Ana Paula Bialer
Bialer Falsetti Associados

Bialer Falsetti Associados (BFA) is a legal and public policy consulting firm established in São Paulo in 2009 as a boutique firm to address the needs of companies in the technology, media and telecommunications industries. The firm also has an office in Brasília to ensure proximity to regulators, policy makers and quick turnaround for clients' needs. Its lawyers have

experience at cutting-edge law firms, legal departments of large companies and government institutions, aiming to provide high quality services in an efficient and personalised way. BFA handles public policy mandates and advises on the regulatory aspects of the technology sector.

Author



Ana Paula Bialer is a lawyer and public policy expert with recognised experience in the areas of technology, telecommunications, and audiovisual media. She is an expert in privacy and data protection, holding CIPP-E

certification from the IAPP (International Association of Privacy Professionals) and a DPO certification from the European Centre on Privacy and Cybersecurity (ECPC) at Maastricht University, where she also holds AI Trust and Safety Officer certification. She is a member of the National Data Protection Council to the ANPD as well as of the National Cybersecurity Committee (CN-Ciber), within the scope of the Chamber of Foreign Affairs and National Defense of the Federal Government Council. She has published books and articles on topics related to her field of expertise.

Bialer Falsetti Associados

Av. Santo Amaro, 3330 - cj 12
Brooklin, São Paulo - SP, 04556-300
Brazil

Tel: +55 11 5102-2297

Web: [linkedin.com/company/bialer-falsetti](https://www.linkedin.com/company/bialer-falsetti)



Introduction

As our lives become more digital, privacy and data protection have increasingly turned into an everyday topics and concerns. In the past decade, the concept of informational self-determination has ceased to be restricted to the world of privacy professionals and has become a topic of dinner-table conversations among friends. These conversations touch basic human rights as well as political decisions by global leaders.

This coming year is set to represent a turning point for privacy and data protection in Brazil. As of 2026, the Brazilian Data Protection Authority, an entity which previously had administrative and financial constraints, has been transformed into a national regulatory body, with technical, administrative and financial autonomy. The Agency will more than double the number of employees dedicated to carrying out its legal mandate. As a result, the responsive approach that has characterised the Agency's activities is likely to gradually evolve to a more robust one, with numerous enforcement activities and potentially heavier sanctions being applied.

Protection of Children

In addition to the transformation of its legal nature, with the increase in both financial and human resources, the Brazilian Data Protection Agency (ANPD) enters 2026 with a new mandate: it has become the organisation within the Federal Administration responsible for enforcing the Brazilian Minors' Online Safety Law, known as the ECA Digital, that was enacted in September 2025.

The centrality of this topic for the Agency's activities is such that the Regulatory Agenda for the 2025–2026 biennium was updated at the end of the year, expanding the agenda to include aspects of the implementation of the ECA Digital, namely:

- age verification mechanisms;
- the scope and general obligations of the ECA Digital applicable to suppliers of information technology products or services; and
- oversight and sanctioning of the ECA Digital, including the revision of existing resolutions around proceedings and enforcement procedures.

The regulatory initiative includes the preparation of a guidance document to clarify the main concepts related to the scope of application of the ECA Digital, as well as the duties applicable to information technology products or services. Additionally, the introduction of interpretative guidelines is important for ensuring a proper understanding of the scope of application of the ECA Digital and providing greater legal certainty for regulated entities in the process of implementing the law. An upcoming guideline will also establish clarifications on the duties of prevention, protection, information, and security, which are some of the most challenging concepts to be defined within the new framework. Establishing boundaries to ensure that organisations are clear on what needs to be done will be critical for the purposes of regulatory compliance.

While there is an international trend towards online safety laws with specific provisions around minors, age verification and assurance mechanisms being increasingly considered and a call for more tools for parent supervision, Brazil seems to have taken the lead with a more structured and comprehensive set of obligations. Time will tell if all these duties can be implemented without substantially disrupting the online experience for both minors and adults.

Priorities for Regulation and Enforcement in Brazil

A map of priorities for 2026–2027 was published by ANPD at the end of the year. This is an important indication as to which areas the ANPD will focus its attention and enforcement initiatives, and therefore where additional caution should be taken by processing agents. Among others, the following key topics were identified.

- Rights of personal data subjects, especially regarding the processing of biometric data: the ANPD has emphasised technical security measures and the underlying legal basis, eg, health and financial data. This has been one of the most challenging topics since the approval of the Brazilian Data Protection Law (LGPD) in 2018 as it raises numerous questions from processors on the correct approach for implementation. Decisions usually involve substantial investments in processes, systems and personal training. Furthermore, specific aspects of the Brazilian market may require regulations that

differ from best practices adopted in other jurisdictions. This year, we can expect enforcement activities related to data subjects' rights in different areas, as well as some related to the secondary use of personal data for the delivery of targeted commercial advertising, especially through profiling techniques.

- Protection of children and adolescents in the digital environment to verify how processors will comply with the requirements of the ECA Digital: in 2026, this will involve inspection activities aimed at verifying the legality of the processing of personal data of these subjects and proposing safeguards to controllers within the scope of inspection activities (such as age verification mechanisms). In 2027, the enforcement activities are expected to expand to include considerations around configuration, by design and by default, of the most protective model available in relation to privacy and personal data protection, including parental supervision tools. A number of now-established industry practices may have to be reviewed to comply with the new standards. Enforcement activities will also look at the adoption of measures to prevent children and adolescents from accessing inappropriate, unsuitable, or legally prohibited content, including age verification mechanisms.
- Processing of personal data by the government: the ANPD will focus on promoting and disseminating greater compliance with the LGPD, especially regarding the sharing of personal data, the adoption of technical safeguards in the management and governance of processed data, and the use of biometric data. Considering that governments are often the largest processors of personal data, clear parameters are central to ensuring compliance with the data protection laws and constitutional principles around fundamental rights, in a much broader sense than the privacy discussion per se. While there is an international trend towards optimising the sharing of data and the use of data for the purpose of generating value and better public policies, the privacy concerns that such sharing, especially of personal data can raise from a privacy perspective cannot be overstated.
- AI and emerging technologies in the context of personal data processing has also been identified as a priority for the ANPD. In addition to the scope

of automated decision-making parameters, in the context of training and use of AI systems, the following will also be reviewed: (i) rights of data subjects; (ii) principles of the LGPD; (iii) legal hypotheses; and (iv) good practices and governance.

AI

AI has increasingly caught the attention of data protection regulators due to its intersection with personal data, even though so much of AI does not involve any personal data. While the ANPD has already established specific proceedings to address the use of personal data in AI training, its legal authority in the AI field is currently limited to the revision of automated decisions or the use of personal data, as that is specifically provided for in the LGPD.

However, there are advanced legislative initiatives to expand the ANPD's legal authority, including it becoming the central co-ordinating body for AI regulation in Brazil. International experience shows that this is not a one-size-fits-all discussion and different institutional arrangements are possible, none of which being the best or the right one. The challenge is to ensure that regulation around AI and data protection do not merge into a single approach as that could hinder the development of AI, and, consequently, the social and economic benefits it can bring.

Data, Competition and Digital Markets

The central role that data plays in the organisation of the economy cannot be overstated and has led to an overlap of important discussions around the role of data, the structure of markets and the power that companies operating in this area have.

As with regulation, the discussions around the need for a Digital Market Act and a Digital Services Act will continue to be a part of the conversation around preparing digital public policies aimed at addressing a new momentum and organisation of the economy and society. Competition authorities will continue to move closer to the data universe, prompting reflections around the role of data from a more structural perspective, rather than from an individual rights approach. Legislative initiatives are less likely to advance in 2026 considering the presidential election

cycle and the world cup, which are likely to divert attention from digital policies, at least for a few weeks.

Cross Border Data Flow

Finally, cross border data flow is one of the most central issues around the world and is always a hot topic, especially given the many geopolitical situations the world currently faces. Data needs to flow freely to ensure international trade, to enable the provision of products and services and for society to develop in a more integrated manner. Brazil starts 2026 with a mutual adequacy decision with the EU; this is long overdue and is expected to bring legal certainty to a number of businesses. While the LGPD establishes data transfer mechanisms similar to those of the GDPR, a number of them were still pending regulation and the market was anxiously waiting for an EU adequacy decision to resolve some of the legal uncertainty. With the decision from the EU, Brazil can now work on expediting adequacy decisions with other jurisdictions, as well as on expediting equivalence decisions for substantially similar contractual clauses.

Final Remarks

While regulation is typically slow and a few steps behind technological development, the coming months are expected to be substantially active in advancing the regulation of the digital environment, particularly in terms of important matters affecting the processing of personal data. A more robust and detailed regulatory framework for the protection of minors online will also be a priority, closely followed by the advancements around the intersection between AI and personal data. The establishment of a regulatory framework on AI will be a long-term project. The goal will be to ensure that regulators are able to incorporate innovation into their oversight, while individual rights are ensured and protected.

CHILE



Law and Practice

Contributed by:

Claudio Magliona, Bárbara Reyes and Diego Lisoni
Magliona Abogados

Contents

1. Legal and Regulatory Framework p.32

- 1.1 Overview of Data and Privacy-Related Laws p.32
- 1.2 Rights and Obligations p.33
- 1.3 Special Categories of Personal Data p.35
- 1.4 Processing of Personal Data for Research and Development Purposes p.36
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.37
- 1.6 Data Breach Requirement p.38
- 1.7 Regulators p.39
- 1.8 Enforcement Proceedings and Fines p.39
- 1.9 Enforcement Trends p.40

2. Privacy Litigation p.40

- 2.1 Privacy Litigation Overview p.40
- 2.2 Recent Case Law p.40
- 2.3 Collective Redress Mechanisms p.41

3. Requirements for the Protection and Processing of Non-Personal Data p.41

- 3.1 Objectives and Scope of Data Regulation p.41
- 3.2 Interaction of Data Regulation and Data Protection p.42
- 3.3 Rights and Obligations Under Applicable Data Regulation p.43
- 3.4 Regulators and Enforcement p.43

4. Sectoral Topics p.43

- 4.1 Use of Cookies p.43
- 4.2 Personalised Advertising and Other Online Marketing Practices p.43
- 4.3 Employment Privacy Law p.44
- 4.4 Data Protection in M&A p.44

5. International Considerations p.44

- 5.1 Restrictions on International Data Transfers p.44
- 5.2 Government Notifications and Approvals p.45
- 5.3 Data Localisation Requirements p.45
- 5.4 Blocking Statutes p.45
- 5.5 Recent Developments p.45

Magliona Abogados specialises in corporate matters, tax services, complex business litigation and finance structures, telecommunications, technology law, intellectual property, and government relations and public policy, including corporate structuring, due diligence planning, M&A, financial assistance, syndicated loans, liability restructuring and leasing. It has expertise in licensing and software development agreements, technological platforms, franchises,

data protection and computer crime, as well as the distribution, production and financing of film and television. The firm's clients encompass a wide range of enterprises, both local and multinational, engaged in banking and finance, technology and software, leasing and insurance. It also counsels public agencies and companies in the movie industry, as well as other diverse fields.

Authors



Claudio Magliona is the founding partner of Magliona Abogados. He has a wealth of experience in data protection, IP and TMT, and an extensive practice in corporate and financing, technology law,

telecommunications, intellectual and industrial property, and entertainment law, including corporate structures, M&A, financing, licensing and software development agreements, franchising, data protection, prevention of computer crimes as well as film distribution, production and financing. Claudio, who also handles government relations and policy matters, has spoken at numerous conferences around Latin America. He is the author of various publications on technology and law, data protection, IP and film financing.



Diego Lisoni is a researcher who joined Magliona Abogados in 2021. Diego focuses on researching corporate, jurisprudential, regulatory and public policy matters. He studied Law at Universidad de Chile and is a teaching assistant in Administrative Law and E-Commerce and New Technologies. In addition, he is a member of the Board of Internet Society Chile Chapter and Community Fellow of Internet Society.



Bárbara Reyes is an attorney and Director of Magliona Abogados. She has a wealth of experience in privacy and data protection, cybersecurity, compliance, fintech services, public affairs and government relations

management. Bárbara has a Diploma in Compliance from the PUCV, and a Postgraduate Diploma in Regulation in the Digital Economy from the Universidad de Chile. In addition, she has an International Certification in Personal Data Protection ALAP-APEP (2024) and certification as a Data Protection Officer and Lead Implementer of ISO 27701.

Magliona Abogados

Santiago de Chile
Avda Andrés Bello 2687
Piso 24, Las Condes
Santiago de Chile
Santiago
Chile

Tel: +56 2 3210 0030
Fax: +56 2 377 9451
Email: contacto@magliona.cl
Web: www.magliona.cl



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Overview of Data and Privacy-Related Laws

The Chilean legal framework for data protection is anchored in Article 19, No 4 of the Political Constitution of the Republic of Chile, which guarantees the protection of personal data. This constitutional provision ensures that the processing and protection of personal data must be carried out in the manner and under the conditions established by law. Additionally, Chile has a specific statute, Law No 19.628 on Privacy Protection (the “Law”), published on 28 August 1999. While the current version of the Law was not originally based on international instruments such as the GDPR, a significant reform has recently been enacted.

On 13 December 2024, Law No 21.719 on Personal Data Protection (the “New Law”) was published in the Official Gazette, reforming and updating Law No 19.628. This regulation introduces substantial modifications and raises standards for data controllers and processors, drawing inspiration from the European Union’s General Data Protection Regulation (GDPR). The New Law establishes a 24-month vacancy period, meaning it will enter into full force on 1 December 2026. During this transition, entities must adapt their processing activities before the new Personal Data Protection Agency (the “Agency”) begins its functions and enforcement powers.

Sectoral Instruments and Interactions Across Levels of Law

Currently, the interaction between legal sources relies heavily on general statutes and sectoral oversight, as there is no centralised data protection authority until the Agency is established in 2026. The interplay between these sources operates as follows:

- **Consumer Protection:** The National Consumer Service (SERNAC) acts as the supervisory body for data protection within consumer relations. SERNAC exercises powers to file class actions, inspect, and issue interpretative circulars, filling the gap until the Agency becomes operational.
- **Public Sector:** The Council for Transparency oversees compliance by state administration bodies. It issues recommendations and manages procedures for access rights (ARCO rights) within the public sector, ensuring co-ordination with the Transparency Law (Law No 20.285).
- **Financial Sector:** The Financial Market Commission (CMF) regulates the financial sector, including data protection and cybersecurity. Under the Fintech Law (Law No 21.521), the CMF is mandated to dictate standards for the Open Finance System. Furthermore, the CMF’s Updated Compilation of Standards (RAN) imposes specific obligations on financial institutions regarding data security and outsourcing.

Extraterritorial Reach

Under the New Law (Law No 21.719), the scope of application extends beyond national borders based on specific triggers designed to protect data subjects located in Chile. The law applies to the processing of personal data when the controller or processor is established in the national territory. Furthermore, strictly extraterritorial application is triggered in the following scenarios:

- when a processor, regardless of their location, performs data processing operations on behalf of a controller established or constituted in Chile;
- when the controller or processor is not established in Chile, but their processing operations are intended to offer goods or services to data subjects located in Chile, regardless of whether payment is required;
- when the processing involves monitoring the behaviour of data subjects located in Chile, including analysing, tracking, profiling, or predicting their behaviour; or
- when a controller not established in Chile is subject to national legislation due to a contract or international law.

Responsible parties not domiciled in Chile who process data of residents must designate an email address or suitable contact method to receive communications from data subjects and the Agency.

Interplay with Non-Personal Data, Cyber, and AI *Cybersecurity and critical infrastructure*

Chile recently enacted the Cybersecurity Framework Law No 21.663, which created the National Cybersecurity Agency (ANCI). This law interacts with data protection statutes by mandating the reporting of cybersecurity incidents that may affect personal data. The law establishes the principle of “security and privacy by default and by design”, requiring systems to be designed with data protection in mind.

Specific interplay includes:

- **Incident Reporting:** Institutions must report incidents with significant effects to the National CSIRT. If an incident affects systems containing personal data, it is considered to have a “significant effect”.

- **Data Protection in Reporting:** Reports of cyber incidents must generally omit personal data to protect privacy, unless essential for management, and IP addresses are explicitly excluded from the definition of personal data for these specific reporting purposes.

Artificial intelligence (AI)

The regulation of AI in Chile is evolving and intersects directly with data privacy rules. The National AI Policy 2024-2031 promotes ethical and responsible AI use.

- **Current Guidance:** Guidelines for state agencies recommend that processing personal data for AI training or development must strictly comply with Law No 19.628, ensuring data is used only for authorised purposes. It is advised not to enter sensitive personal data into generative AI tools not contracted by the state.
- **Legislative Proposals:** A bill regulating AI systems is under discussion, inspired by the EU AI Act. This bill proposes a risk-based approach and establishes that the new Personal Data Protection Agency will act as the supervisory authority for AI matters, while a Technical Advisory Council and the Ministry of Science will handle regulatory powers.
- **Automated Decisions:** The New Law introduces the right for data subjects not to be subject to decisions based solely on automated processing, including profiling, that produce legal or significant effects.

1.2 Rights and Obligations

General Principles and Requirements for Processing

The Chilean legal framework regarding personal data is currently undergoing a significant transition following the publication of Law No 21.719 (the “New Law”) on 13 December 2024, which updates Law No 19.628. This regulation introduces a comprehensive catalogue of principles that align Chile with international standards, particularly the GDPR.

Principles of Data Processing

Under Article 3 of the New Law, any processing of personal data must strictly adhere to the following principles:

- **Lawfulness and Loyalty:** Data must be processed lawfully and fairly, and the controller must be able to prove the lawfulness of the processing.
- **Purpose:** Data must be collected for specific, explicit, and lawful purposes and cannot be processed for different objectives, unless they are compatible with the original purpose or authorised by the data subject.
- **Proportionality:** Data processing must be limited to what is necessary, suitable, and relevant for the specific purposes.
- **Quality:** Data must be accurate, complete, current, and relevant.
- **Security:** The data controller must guarantee adequate security standards to protect data against unauthorised access, loss, leakage, or destruction.
- **Transparency and Information:** Controllers must provide clear and accessible information regarding their data processing policies and practices to the data subjects.
- **Confidentiality:** Controllers and anyone with access to data must maintain secrecy, a duty that persists even after the relationship with the data subject ends.
- **Accountability:** Those processing data are legally responsible for complying with these principles and obligations.

Requirements for Processing (Lawful Bases)

For data processing to be lawful, it must rely on a valid legal basis. While consent is the general rule, it is not the only basis for processing.

- **Consent:** It must be free, informed, specific, and unequivocal, given through a clear affirmative action or declaration.
- **Contractual Necessity:** Processing is permitted if necessary for the conclusion or execution of a contract between the data subject and the controller.
- **Legal Obligation:** Processing is allowed when necessary to comply with a legal obligation.
- **Legitimate Interest:** Data may be processed to satisfy the legitimate interests of the controller or a third party, provided this does not override the rights and freedoms of the data subject.

Data Subject's Rights

The New Law significantly expands the rights of individuals, enhancing their control over their personal information. These rights are personal, non-transferable, and cannot be waived.

- **access** – the right to obtain confirmation from the controller about whether their data is being processed and to access specific information about the processing, such as purposes and recipients;
- **rectification** – the right to request the modification or completion of data that is inaccurate, outdated, or incomplete;
- **suppression (deletion)** – the right to request the elimination of data when, for example, it is no longer necessary for the collected purpose or when consent is revoked;
- **opposition** – the right to object to specific processing activities, particularly when based on legitimate interest or for direct marketing purposes;
- **portability** – the right to receive a copy of provided personal data in a structured, commonly used, and machine-readable format to transfer it to another controller;
- **blocking** – the right to request the temporary suspension of any processing operation on the stored data; and
- **automated decisions** – the right not to be subject to decisions based solely on automated processing, including profiling, which produce legal effects or significantly affect the individual.

Compliance “To-Dos” for Organisations

As the New Law creates a 24-month vacancy period before full enforcement begins in December 2026, organisations must utilise this time to adapt their internal processes. The following steps are essential to ensure compliance and mitigate the risk of severe sanctions:

- **Conduct a Gap Analysis and Data Mapping:** It is highly advisable to perform a comprehensive diagnosis to identify the current state of their data processing activities compared to the new regulatory standards. This involves creating a Record of Processing Activities (RAT) to identify the types of data treated (especially sensitive data), the lawful basis for each processing activity, and data flows.

- **Implement an Infringement Prevention Model:** It is highly advisable to adopt an Infringement Prevention Model (Compliance Programme) that can then be certified by the Agency, which will reduce the amount of penalties for possible infringements. This model must include the appointment of a data protection officer (DPO) who will act as a point of contact between the authority and the interested parties. The DPO must have sufficient resources and independence to perform their duties effectively.
- **Update Policies and Contracts:** Privacy policies must be updated to meet the new transparency requirements, clearly explaining rights and legal bases to data subjects. Furthermore, all contracts with third-party service providers (data processors) must be reviewed and updated to include specific mandatory clauses regarding confidentiality, security, and the prohibition of using data for other purposes.
- **Risk Management and Security Measures:** Organisations must implement technical and organisational security measures appropriate to the risk, such as encryption or pseudonymisation. For processing activities that pose a high risk to data subjects' rights, performing a Data Protection Impact Assessment (DPIA) is mandatory prior to processing.
- **Establish Incident Response Procedures:** Procedures must be established to detect, manage, and report security breaches. The New Law imposes a duty to report security breaches to the Data Protection Agency and, in certain cases involving high risk, to the affected data subjects.
- **Manage International Transfers:** If the organisation transfers data outside of Chile, it must ensure the destination country offers adequate protection or implement appropriate guarantees, such as standard contractual clauses approved by the Agency. Without these guarantees, international transfers may constitute a serious infringement.

1.3 Special Categories of Personal Data

Based on Law No 21.719 (the "New Law"), which modifies Law No 19.628, the Chilean legal framework establishes a reinforced protection regime for specific categories of data. These rules impose stricter obliga-

tions on data controllers compared to the processing of standard personal data.

Sensitive Data

The New Law defines sensitive data as information referring to the physical or moral characteristics of individuals, or facts regarding their private life or intimacy. This includes data revealing ethnic or racial origin, political affiliation, union membership, socio-economic situation, ideological or philosophical convictions, religious beliefs, health, biological profiles, biometrics, and information regarding sexual life, orientation, or gender identity.

General rule for processing

The processing of sensitive data is generally prohibited unless the data subject provides their express consent. This consent must be given through a written declaration, verbally, or via an equivalent technological medium.

Exceptions to consent

The legislation provides specific legal bases where sensitive data may be processed without consent, provided it is done lawfully:

- **Publicly Available Data:** Sensitive data may be processed without consent when the data subject has made the data manifestly public, and the processing aligns with the purpose of that publication.
- **Non-Profit Associations:** Foundations, NGOs, or associations with political, philosophical, religious, or trade union aims may process data of their members. This is permissible provided the processing relates solely to their members, guarantees are in place to prevent leaks, and the data is not transferred to third parties.
- **Vital Interests:** Sensitive data may be processed without consent when necessary to safeguard the life or physical/psychic integrity of the holder or another person, particularly if the data subject is physically or legally unable to consent.
- **Legal Defence:** Sensitive data may be processed without consent when necessary for the formulation, exercise, or defence of a right before courts or administrative bodies.

Health, Biological, and Biometric Data

The regulation creates a sub-category for health and biological data (such as genetic or metabolic profiles), which generally follows the rules for sensitive data but includes specific sanitary exceptions. These may be processed without consent for reasons of public health interest (such as sanitary alerts), medical diagnosis, provision of healthcare services, or scientific research, provided the data is anonymised prior to any publication of results.

Regarding biometric data (fingerprints, iris scans, voice, facial features), the controller must comply with heightened transparency duties. Before processing, the controller is obliged to inform the data subject about the specific identification system used, the precise purpose, the duration of the use, and the method for exercising data subject rights.

Data Relating to Minors (Children and Adolescents)

The New Law introduces a regime based on the principle of the best interest of the child and progressive autonomy. It distinguishes between “children” (under 14 years old) and “adolescents” (14 to under 18 years old).

- Children (Under 14): Processing requires the express consent of their parents, legal representatives, or those holding personal care. There is no scenario where a child under 14 can validly consent on their own.
- Adolescents (14 to 17): Generally, adolescents may provide consent for the processing of their data autonomously. However, if the data is classified as sensitive, adolescents under the age of 16 still require the consent of their parents or legal guardians.

Educational establishments and other entities processing data of minors have a specific statutory obligation to ensure the lawful use and protection of this information.

1.4 Processing of Personal Data for Research and Development Purposes

Anonymisation of Patient Data for Research and Development

Under the Chilean legal framework, particularly following the enactment of Law No 21.719 (the “New Law”) which updates Law No 19.628, the processing of health data is subject to a reinforced protection regime. However, specific provisions allow for the use and anonymisation of such data for scientific and product development purposes under strict conditions.

Exceptions for Scientific Research and Product Development

While the general rule for processing sensitive data (such as health data) is the requirement of express consent from the data subject, the legislation introduces specific exceptions relevant to life sciences companies:

- Public Interest and Human Health Benefit: Processing health and biological profile data without consent is permitted when used for historical, statistical, or scientific purposes. This specifically includes studies or investigations that serve the public interest or benefit human health, as well as the development of medical products or inputs that could not be developed otherwise.
- Legitimate Interest in Research: The law establishes a presumption of legitimate interest for processing performed exclusively for historical, statistical, or scientific purposes, provided they serve the public interest.
- Requirement to Anonymise for Publication: While the processing for the research itself may involve personal data under strict security measures, the New Law mandates that any publication or diffusion of the results and analyses obtained from such studies must be preceded by the anonymisation of the data.

Mandatory Data Protection Impact Assessments (DPIAs)

Life sciences companies will likely be required to conduct a DPIA prior to commencing processing. The New Law mandates this assessment when processing is likely to result in a high risk to data subjects’

rights, explicitly listing the processing of sensitive data (health data) as a trigger for this obligation.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

The intersection of artificial intelligence (AI) and data privacy in Chile is currently governed by the recently enacted Law No 21.719 (the “New Law”), which updates Law No 19.628, and a series of sectoral guidelines. While a specific bill regulating AI systems is under discussion in Congress, the New Law establishes the binding framework for processing personal data within AI models.

General Requirements and Specific Guidance

The use of personal data in AI systems must adhere to the general principles of the New Law, such as purpose limitation, proportionality, and security. There are specific requirements regarding automated decision-making and profiling, which are now formally regulated.

In terms of guidance, distinct bodies have issued soft law instruments:

- **Public Sector:** The Ministry of Science and the Digital Government Division issued a Circular Letter with “Recommended Guidelines for the Use of AI by State Agencies”. It explicitly advises against entering sensitive personal data into generative AI tools unless they have been contracted or developed specifically for the agency with appropriate safeguards.
- **Consumer Protection:** The National Consumer Service (SERNAC) issued an interpretative circular regarding AI in consumer relations. It establishes that companies must ensure transparency, avoid arbitrary discrimination, and strictly protect consumers’ personal data when deploying AI systems.

Rules Governing Automated Decision-Making

The New Law introduces a specific regime for automated decision-making (ADM), granting data subjects significant control over how AI affects them.

Right to opposition and explanation

Data subjects have the right not to be subject to decisions based solely on the automated processing of

their personal data, including profiling, if those decisions produce legal effects or significantly affect them.

Exceptions and safeguards

ADM is permissible only under three specific circumstances:

- it is necessary for the conclusion or execution of a contract;
- it is authorised by law (with specific safeguards); or
- the data subject has granted their express consent.

Even when these exceptions apply, the controller must implement suitable measures to safeguard the data subject’s rights. These include the right to obtain human intervention, to express their point of view, to receive an explanation of the decision, and to challenge it.

Risk-Based Regime and High-Risk Categories

The Chilean framework is increasingly shifting towards a risk-based approach, both under the data protection regime and the proposed AI legislation.

Mandatory Impact Assessments for AI

Under the New Law, the regime is risk-based. Controllers must conduct a Data Protection Impact Assessment (DPIA) prior to processing if the activity is likely to result in a high risk to the rights of data subjects. The law explicitly categorises the following AI-related activities as mandatory cases for a DPIA:

- systematic and exhaustive evaluation of personal aspects based on automated processing, including profiling, that produces legal or significant effects; and
- massive data processing or processing on a large scale.

Proposed AI regulation

A bill regulating AI systems, currently before the Senate, proposes a risk classification system inspired by the EU AI Act. It categorises AI systems into unacceptable (prohibited) risk, high risk, limited risk, and no evident risk.

Impact on Transparency, Governance and Oversight

- **Transparency and Information:** The New Law mandates a duty of active transparency. Controllers engaging in ADM or profiling must provide the data subject with “significant information” about the logic applied, as well as the significance and the envisaged consequences of such processing for the individual.
- **Data Governance:** The pending AI bill proposes establishing a principle of data governance, translating into specific obligations for operators of high-risk AI systems regarding information management. Furthermore, the public sector guidelines emphasise interoperability and preventing the misuse of data in generative AI tools not under direct state control.
- **Human Oversight:** The requirement for “human intervention” is a statutory right under the New Law for any ADM process.

1.6 Data Breach Requirement

Requirements Applicable in Case of a Data Breach

Under the new regulatory landscape established by the New Law, the management of security incidents has shifted from a reactive, unregulated approach to a proactive, mandatory reporting regime.

The duty to report to the Agency

The New Law introduces a statutory obligation for data controllers to report security breaches to the Agency. This duty arises when a breach of security measures results in the destruction, leakage, loss, or accidental or unlawful alteration of personal data, or unauthorised access to such data.

- **Trigger:** The obligation applies specifically when the breach poses a reasonable risk to the rights and freedoms of the data subjects.
- **Timing:** The report must be made through the most expeditious means possible and without undue delay.
- **Content:** The notification must describe the nature of the breach, the effects, the approximate number of affected data subjects, and the remedial measures taken.

The duty to notify data subjects

In addition to notifying the regulator, the controller must communicate the breach directly to the affected individuals in specific high-risk scenarios. This notification is mandatory when the breach involves:

- sensitive personal data (such as health or biometric data);
- data relating to minors (children and adolescents); or
- data regarding economic, financial, banking, or commercial obligations.

This communication must use clear and simple language, detailing the specific data affected, the potential consequences, and the safeguard measures adopted. If individual notification is not feasible, the controller must publish a notice in mass media with national reach.

Necessary Action Items for Organisations

- **Detection and Internal Recording:** The organisation must immediately log the incident. The New Law requires the maintenance of a register of breaches, documenting the nature of the event, its effects, and the categories of data affected. This internal record is essential for demonstrating compliance to the Agency during future audits.
- **Mitigation and Containment:** Controllers must deploy immediate technical and organisational measures to reduce the impact of the breach. For entities classified as Operators of vital importance under the Cybersecurity Framework Law, specific regulations mandate actions such as restricting access to compromised systems, isolating affected networks, and changing administrative passwords within three hours of detection.
- **Risk Assessment:** The Data Protection Officer (DPO) or the security team must evaluate whether the breach poses a “reasonable risk” to the rights and freedoms of individuals to determine if notification to the Agency is required.
- **Management of Data Processors:** If the breach originated from a third-party service provider (data processor), the provider has a statutory obligation to report the incident to the controller. Organisations must ensure their contracts explicitly man-

date this reporting to allow the controller to meet its own regulatory deadlines.

Mass Data Privacy Litigation

The breach of the duty to report or the failure to implement adequate security measures can trigger significant civil liability. The New Law expressly establishes that the controller must indemnify both patrimonial and non-patrimonial (moral) damages caused to data subjects.

- **Class Actions:** While individual lawsuits are possible, the most significant risk lies in collective redress mechanisms. SERNAC or consumer associations can file class actions (*demandas colectivas*) representing the collective interest of consumers affected by a mass data breach.
- **Compensation:** The law allows for the indemnification of damages once the administrative sanction is final.

Please note that privacy litigation is dealt with in greater detail in **2. Privacy Litigation**.

1.7 Regulators

At present, and in general, the main regulators of data protection are the civil courts under the Law. However, this will change in 2026 when the Personal Data Protection Agency created by the New Law begins operating.

For its part, currently other entities have powers in matters of personal data protection, the main ones being the following.

Consumer Rights

Currently, the National Consumer Service (SERNAC) is the supervisory body for the protection of personal data in the context of consumer relations, until the Personal Data Protection Agency is established in 2026.

Although it does not have sanctioning powers, SERNAC can exercise its powers to file individual or class actions before the courts, supervise, inspect, investigate, and issue interpretative circulars that are mandatory for SERNAC officials when applying the regulation and the Law (eg, at the time of audit).

Public Sector

The Council for Transparency is responsible for ensuring compliance with the Law by the organs of state administration. The Council has issued the Recommendations on Protection of Personal Data by the Organs of the State Administration, the Guide on Protection of Personal Data for Public Institutions (2021).

Financial Sector

The Financial Market Commission (CMF) is the control body in the financial sector and has regulatory and supervisory powers in matters of personal data protection, information security and cybersecurity.

Under Chapters 18-5, on information about debtors from financial institutions, and Chapters 20-6 and following the Updated Compilation of Standards (RAN) of the CMF on business continuity, information security and outsourcing of services, financial institutions must have an internal policy on security and management of debtor information (PISMID), which must follow international principles and best practices on personal data processing.

Law No 21.521, known as the “Fintech Law”, to “[promote] competition and financial inclusion through innovation and technology in the provision of financial services”, mandates the CMF to dictate the cybersecurity and personal data protection standards that financial institutions participating in the future Open Finance System must comply with.

Cybersecurity

In the area of cybersecurity, Chile has the Cybersecurity Framework Law No 21.663, which created the National Cybersecurity Agency. In terms of personal data protection, the Cybersecurity Framework Law considers the obligation of essential service providers and operators of vital importance to report cybersecurity incidents with significant effects to the National CSIRT, including incidents affecting computer systems containing sensitive personal data.

1.8 Enforcement Proceedings and Fines

There is currently no privacy regulator or data protection authority in Chile. Data protection enforcement is addressed by general courts with general powers. A summary court procedure is established by the Law

if the person responsible for the personal data registry or bank fails to respond to a request for access, rectification, suppression or blocking of personal data within two business days or refuses a request on grounds other than the security of the nation or the national interest.

On the other hand, the New Law moves from a judicial framework to an administrative one, where the body in charge of overseeing this new regulatory standard will be the Personal Data Protection Agency, an administrative body of a technical nature, with regulatory, interpretive, supervisory and sanctioning powers.

With regard to penalties, in the event of non-compliance with the Law, the Agency may:

- issue warnings or impose fines of up to 5,000 UTM for minor infringements; up to 10,000 UTM for serious infringements; and up to 20,000 UTM (or up to approximately USD1.5 million) for very serious infringements;
- triple the fines in the event of repeat offences;
- in the case of large companies, the fine may reach the higher of the tripled fine or up to 2% or 4% of annual income in the event of repeat serious or very serious offences, respectively;
- suspend data processing for up to 30 days as an additional penalty in the case of fines imposed for repeated very serious infringements within 24 months; or
- administer the National Registry of Penalties and Compliance (whose entries will be publicly accessible for five years), which will record the persons responsible for the penalties and the respective penalties.

1.9 Enforcement Trends

Over the past 24 months, Chile has witnessed a discernible rise in litigation related to privacy and personal data protection, driven largely by public debate surrounding the collection and use of biometric data. The high-profile case of WorldCoin, an entity scanning individuals' irises in exchange for cryptocurrency, exemplifies this trend and has triggered actions from both private citizens and public bodies. Additionally, there is a growing tension between distinct public interests, as seen in disputes where data privacy prin-

ciples, such as proportionality, are invoked to oppose information requests from other state authorities like the National Economic Prosecutor's Office (FNE).

2. Privacy Litigation

2.1 Privacy Litigation Overview

Claimant Types and Causes of Action

Claimants generally fall into two categories: individual data subjects exercising constitutional protection actions or habeas data remedies, and public bodies acting within their competencies.

- **Individual Claimants:** Individuals typically file protection actions (*recursos de protección*) alleging the violation of their constitutional right to privacy (Article 19 No 4 of the Constitution). Recent causes of action focus on the lack of informed consent for biometric scanning and the difficulty in exercising the right to suppression (deletion) of data.
- **Institutional Claimants:** The National Consumer Service (SERNAC) has taken a proactive role, filing complaints against companies for questionable data collection practices and insufficient information provided to consumers. Conversely, universities have acted as claimants/defendants in resisting data transfer requests from the FNE, arguing that such transfers violate the principle of proportionality.

2.2 Recent Case Law

SERNAC v WorldCoin

- The National Consumer Service (SERNAC) has initiated legal action against WorldCoin, a company that scans people's irises in exchange for cryptocurrency, for alleged violations of the Consumer Law and the Privacy Law.
- SERNAC argues that WorldCoin has failed to adequately inform consumers about the purposes for which their biometric data will be used and that the company has not implemented appropriate mechanisms to protect consumer privacy.
- SERNAC has also expressed concern that WorldCoin has scanned the irises of minors without the consent of their parents or guardians.

- SERNAC has asked the courts to suspend WorldCoin operations in Chile until it is proven that the company complies with regulations.

Universities v FNE

- The National Economic Prosecutor's Office (FNE) has faced opposition from three universities (PUC, USACH, and University of Chile) when requesting student contact information for a market study on higher education.
- Universities argue that the FNE does not have the authority to request personal data from students (since this requires express legal authorisation according to the current Law 19,628), and that doing so would affect their right to privacy, and that this would violate the principle of proportionality in the processing of personal data.
- The FNE defends its competence to request the information, arguing that it is necessary for the market study and that Law No 20.945 grants it the power to require information from individuals.

Sánchez v WorldCoin

- In this case, the Court of Appeals of Valparaíso rejected the protection action filed by a man against WorldCoin. The ruling was confirmed by the Supreme Court in December 2024.
- The Court argued that the plaintiff consented to the scanning of his iris in exchange for cryptocurrency and that concerns about data storage on the blockchain should be resolved through the specific procedures established in Law No 19.628 (eg, right to suppression of personal data).

2.3 Collective Redress Mechanisms

The National Consumer Service (SERNAC) could bring collective actions on behalf of the collective or diffuse interest of consumers before courts.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation General Legal Framework for Non-Personal Data

Unlike the European Union, Chile does not currently have a single, comprehensive piece of legislation equivalent to the EU Data Act that governs cross-

sector access and sharing of non-personal data. There is no unified statutory regime dedicated solely to industrial data, non-personal IoT data, or the commercial exchange of data between private entities.

Instead, the regulation of non-personal data is fragmented across various sectoral laws and technical standards, focusing primarily on cybersecurity, public sector interoperability, and financial stability.

Public Sector Data Management and Interoperability

While a unified law is absent, there is significant legislative and regulatory activity regarding data governance within the state, which directly impacts private sector providers.

The National Public Sector Data Management System

Discussions are currently underway regarding a legislative proposal establishing the National Public Sector Data Management System. This initiative seeks to create a robust governance framework for data held by the state.

- Secondary Regulations: The implementation of such a system implies the enactment of numerous secondary regulations to define technical standards.
- Impact on Private Providers: This framework will significantly impact private entities providing services to the state, particularly regarding interoperability. Private vendors interacting with public bodies will be required to align their technical standards with government protocols to ensure seamless data exchange and security.

Digital Transformation Law

This move towards a data-driven state is supported by Law No 21.180 on the Digital Transformation of the state. This law mandates that administrative procedures be expressed through electronic media.

- Interoperability: Public bodies must achieve a high degree of interoperability to avoid duplicating information requests to citizens.
- Technical Standards: Decree No 7/2023 establishes technical standards for information security and

cybersecurity, requiring public bodies to implement processes that safeguard confidentiality, integrity, and availability of information (both personal and non-personal) on their electronic platforms. There are other regulations establishing rules for interoperability, authentication, etc.

Cybersecurity and Critical Infrastructure

The protection of non-personal data is addressed through the lens of cybersecurity and critical infrastructure protection.

Cybersecurity Framework Law (Law No 21.663)

This law, which entered into force in 2024, applies to both public and private entities providing “essential services” (eg, energy, telecommunications, finance, digital infrastructure).

- **Scope:** The law protects the resilience of networks and computer systems. It mandates the reporting of incidents that could have “significant effects” on the continuity of essential services, regardless of whether personal data is compromised.
- **Regulated Actors:** The National Cybersecurity Agency (ANCI) regulates “Operators of Vital Importance” (OIV). These operators must implement security management systems to protect their information assets and ensure business continuity.
- **Cloud and Digital Infrastructure:** The ANCI has identified critical digital functions, including data hosting, cloud administration (IaaS, PaaS, SaaS), and data processing services, as falling within the scope of the law due to their importance for national digital infrastructure.

Sectoral Guidance: Financial Services and Cloud Computing

Financial Market Commission (CMF) Rules

The CMF issues binding instructions, such as Chapter 20-7 of the Updated Compilation of Standards (RAN) and General Norms.

- **Cloud Outsourcing:** Financial entities outsourcing data processing to cloud providers must ensure the provider maintains adequate security mechanisms (physical and logical) to isolate the entity's infrastructure from other clients.

- **Data Integrity and Availability:** The regulations require measures to prevent information leaks or events affecting the availability, confidentiality, and integrity of the entity's data.
- **Encryption:** Entities must use encryption techniques for data stored in the cloud, appropriate to the nature and sensitivity of the information.

National Data Centres Plan

To foster the non-personal data economy, the Ministry of Science launched the National Data Centres Plan 2024-2030. This policy aims to promote the growth of the local data centre industry, strengthen connectivity (eg, Humboldt submarine cable), and simplify the permitting process for digital infrastructure projects, thereby facilitating the processing capabilities required for AI and cloud computing.

3.2 Interaction of Data Regulation and Data Protection

Legal Basis and Lawfulness of Processing

The interaction between data regulation frameworks and privacy rules in Chile is fundamentally governed by the principle of lawfulness established in the new Personal Data Protection Law (Law No 21.719). Under this regime, the processing of personal data is only legitimate when founded on specific legal bases, such as the consent of the data subject, the execution of a contract, compliance with a legal obligation, or the satisfaction of legitimate interests. The Cybersecurity Framework Law (Law No 21.663) explicitly states that any data processing carried out for cybersecurity purposes must strictly comply with Law No 19,628 (and its successor, Law No 21.719), particularly regarding the principle of purpose limitation.

Confidentiality of Personal Data

Confidentiality is a transversal obligation across Chilean digital regulations. The Personal Data Protection Law imposes a duty of secrecy and confidentiality on data controllers and processors, a duty that persists even after the relationship with the data subject has ended. In the public sector, officials dealing with sensitive data or infraction records are subject to strict secrecy obligations, where violations are considered grave breaches of administrative probity. Similarly, the Fintech Law (Law No 21.521) mandates that financial information service providers must maintain confiden-

tiality and implement security measures to prevent unauthorised access or disclosure.

Intellectual Property and Non-Personal Data

Regarding non-personal data and intellectual property (IP), the regulatory framework seeks to balance transparency with the protection of proprietary assets. The Cybersecurity Framework Law obliges service providers to share information on vulnerabilities and incidents to prevent cyber threats; however, contracts regarding these services cannot restrict this communication unless it compromises IP protection. Furthermore, legislation on open finance and algorithmic transparency protects the “business secrets” and proprietary logic of algorithms while requiring sufficient information to be provided to the data subject regarding the consequences of automated decisions.

3.3 Rights and Obligations Under Applicable Data Regulation

Interoperability and Data Sharing Conditions

Obligations regarding data sharing and interoperability are particularly strong in the public sector and the fintech ecosystem. The State Digital Transformation Law (Law No 21,180) and the new Data Protection Law mandate state bodies to achieve high levels of interoperability to prevent duplicating requirements for citizens. For private entities, specifically within the Open Finance System, participants must implement Application Programming Interfaces (APIs) that ensure secure and standardised data exchange. These exchanges require express, informed, and specific consent from the client, which can be revoked at any time.

3.4 Regulators and Enforcement

Competent Authorities

The enforcement landscape in Chile is transitioning towards a model with specialised technical authorities. The Personal Data Protection Agency, created by Law No 21.719, is the independent corporation responsible for supervising compliance, interpreting regulations, and sanctioning infringements regarding personal data.

In parallel, the National Cybersecurity Agency (ANCI) enforces the Cybersecurity Framework Law, supervising essential service providers and critical infrastruc-

ture. For the financial sector, the Financial Market Commission (CMF) retains jurisdiction over fintechs and banks, enforcing operational resilience and data protection standards specific to that industry.

Role of the Digital Government Secretariat

Regarding the public sector, the Digital Government Secretariat, which operates under the Ministry of Finance, plays a pivotal role. This entity serves as the intersectoral co-ordinator for the strategic use of digital technologies and data within the State Administration. It is empowered to issue circulars, technical guidelines, and directives to support public bodies in implementing data protection and information security standards.

4. Sectoral Topics

4.1 Use of Cookies

Under both the current law and the New Law that will come into force in December 2026, if cookies collect personal data, they can be considered data processing, so companies that place cookies will require the consent of the data subject (with some exceptions or using other bases of lawfulness of data processing) and comply with the general rules for the processing of personal data.

4.2 Personalised Advertising and Other Online Marketing Practices

Law No 19,496 on the Protection of Consumer Rights contains a provision regarding marketing through email. Every promotional or advertising communication sent by email must indicate its subject, the identification of the sender and a valid email address to which the recipient can address their request for the suspension of the advertising communication, which will remain banned from then on.

Providers that direct promotional or marketing communications to consumers via mail, fax, telephone calls or messaging services must indicate an expedited way the addressees may request the suspension of the communications.

Regarding data privacy, this practice requires consent from the data subject, unless the data comes from sources available to the public.

4.3 Employment Privacy Law

The Political Constitution of the Republic of Chile guarantees the respect and protection of the privacy and honour of a person and their family at a constitutional level. Such constitutional protection extends to workers. The same protection is guaranteed in Article 5 of the Chilean Labour Code.

According to the Labour Department of Chile, employers may regulate the conditions, frequency and timeliness of use of the company's emails, but may not, under any circumstances, have access to the private email correspondence sent and received by employees. This would violate the fundamental rights granted by the Political Constitution of the Republic of Chile.

If there is a breach of a worker's privacy, and that worker is part of a union, the union may apply some pressure on the employer to fulfil the Law.

All means to control workers – including cybersecurity tools – must comply with respect for the fundamental rights granted by the Political Constitution of the Republic of Chile, the right to privacy, a private life and the honour of workers. Therefore, control mechanisms are only allowed if they fulfil the following requirements:

- They must necessarily be incorporated in the normative text that the law establishes for the effect, that is, the Internal Regulations of Hygiene and Safety of the company, dictated in conformity with the law.
- They may only be carried out by suitable means consistent with the nature of the employment relationship.
- The application of control mechanisms must be general, and the impersonality of the measure must be guaranteed (ie, it must not be discriminatory).
- The dignity of the worker must be respected.

4.4 Data Protection in M&A Competition Law Considerations

The National Economic Prosecutor's Office (FNE) reviews concentrations where data accumulation may affect competition. The combination of information assets, such as consumer databases and preferences, can create barriers to entry that weaken competition. Furthermore, the FNE evaluates whether a merger might degrade non-price variables, such as the terms of use or privacy policies applicable to users.

Asset Deals and Transfer of Databases

In asset deals, the transfer of a customer database from the seller to the buyer is legally classified as a "cession" of data.

Requirements for Cession

Under the current regime, the general rule is that personal data may only be processed (which includes transferring) when the law authorises it or the data subject consents. However, the New Law expands the bases for lawfulness. Future transfers may be justified if they are necessary for the execution of a contract between the data subject and the controller, or for the satisfaction of legitimate interests, provided these do not override the rights of the data subject.

Once an asset deal is closed, the status of the parties regarding the data changes.

New Controller Status

Upon the perfection of a data cession, the New Law establishes that the assignee (buyer) acquires the status of "data controller" for all legal effects. The assignor (seller) retains responsibility for any processing they continue to perform. If a cession occurs without necessary consent, it may be deemed void, obliging the buyer to delete the data.

5. International Considerations

5.1 Restrictions on International Data Transfers

At present, the Law does not contain a specific provision in respect of international data transfers. However, the transfer of personal data outside the jurisdiction may be deemed a use of data, for which authorisation

and other requirements established by the Law would therefore be required.

However, the New Law has a chapter dedicated to the international transfer of personal data, contemplating a wide catalogue of cases that would allow data transfers to be carried out under a dynamic framework. See **5.5 Recent Developments**.

5.2 Government Notifications and Approvals

No government notifications or approvals are required to transfer data internationally.

For its part, according to the New Law, it is not necessary to request authorisation from the Personal Data Protection Agency to carry out an international transfer of data, except when some of the specific requirements under which it is legal to carry out this type of activity have not been met.

5.3 Data Localisation Requirements

Currently, the Law does not establish data localisation requirements, nor does the New Law provide for such limitations.

However, under Chapter 20-7 of the Updated Compilation of Standards (RAN) on the outsourcing of services by financial institutions (especially banks), the data, technological platforms, and applications to be used in the outsourcing of services must be located at specific processing sites, and in the case of processing abroad, in a defined and known jurisdiction. In addition to jurisdiction, the city where the data centres operate is also required to be known.

For the purpose of contracting any type of service through the modality called cloud computing, the board of directors of a financial institution must annually determine the level of risk tolerance that the financial institution is willing to assume in this type of outsourcing. This pronouncement must consider an analysis of the data to be stored or processed under this modality and its location.

Without prejudice to the due fulfilment of the different requirements contained in Chapter 20-7, financial institutions may outsource their non-critical services to the public or private cloud. If the financial institu-

tion evaluates the contracting of a cloud service for an activity considered strategic or critical, this may also be carried out in public or private cloud mode. However, in these cases, the financial institution must carry out enhanced due diligence of the provider and the service.

5.4 Blocking Statutes

There are no blocking statutes in Chile.

5.5 Recent Developments

The New law, which will come into force in December 2026, regulates international transfers of personal data in a specific manner, unlike the current Law in force. Thus, international data transfers will be legal in the following cases:

- When the recipient of the data is in a country with adequate levels of data protection.
- When the transfer is covered by contractual clauses or other legal instruments.
- When the data controller and the recipient adopt a compliance model or certification mechanism.

In the absence of an adequacy decision or adequate guarantees, a specific and unusual transfer may be made in the following cases:

- express consent of the data owner;
- bank, financial or stock market transfers;
- compliance with international obligations;
- international judicial co-operation;
- conclusion or execution of a contract; and
- urgent measures in medical or health matters.

The Personal Data Protection Agency will be responsible for determining which countries have adequate levels of data protection. A country's legal system will be deemed to have adequate levels of data protection when it meets standards similar to or higher than those of Chile, taking into account at least whether the country has established principles governing the processing of personal data; the existence of regulations that recognise and guarantee the rights of data subjects and the existence of a supervisory authority; the imposition of information and security obligations; and the establishment of an infringement and liability regime.

The Agency may approve model clauses and other legal instruments only if they contain adequate guarantees for the cross-border flow of data, and will not require any other additional guarantee or authorisation.

When the transfer is made between companies or entities belonging to the same business group, related companies or companies subject to the same controller under the terms provided for in the Securities Market Law, provided that all of them operate under the same standards and policies regarding the processing of personal data, the transfers may be covered by binding corporate rules previously approved by the Agency.

The Agency may authorise in very exceptional cases, by means of a resolution, the international transfer of data for a particular case, provided that the transmitter and the recipient of the data provide the appropriate guarantees.

Adoption of Standard Contractual Clauses

To address the period of legal uncertainty before the New Law fully enters into force, the Ministry of Economy has issued a Resolution approving Standard Contractual Clauses (SCCs) for international transfers. These clauses are based on the models developed by the Ibero-American Data Protection Network (RIPD) and are intended to provide legal certainty and a compliance mechanism for responsible parties during the transition period. These clauses cover transfers between controllers and from controllers to processors.

Potential Acceleration of the Agency's Installation

Although the New Law is scheduled to enter into full force in December 2026, a legal reform is currently under discussion (Bulletin No 18036-05) that proposes modifying the deadlines for the appointment of the Council of the Personal Data Protection Agency. If approved, this reform would allow the President of the Republic to propose Council members to the Senate earlier than originally planned, enabling the Agency to exercise necessary functions for its installation and operational preparation before the general entry into force of the law in late 2026.

Law and Practice

Contributed by:

Jihong Chen

Zhong Lun Law Firm

Contents

1. Legal and Regulatory Framework p.49

- 1.1 Overview of Data and Privacy-Related Laws p.49
- 1.2 Rights and Obligations p.50
- 1.3 Special Categories of Personal Data p.50
- 1.4 Processing of Personal Data for Research and Development Purposes p.51
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.51
- 1.6 Data Breach Requirement p.52
- 1.7 Regulators p.52
- 1.8 Enforcement Proceedings and Fines p.53
- 1.9 Enforcement Trends p.54

2. Privacy Litigation p.55

- 2.1 Privacy Litigation Overview p.55
- 2.2 Recent Case Law p.55
- 2.3 Collective Redress Mechanisms p.55

3. Requirements for the Protection and Processing of Non-Personal Data p.56

- 3.1 Objectives and Scope of Data Regulation p.56
- 3.2 Interaction of Data Regulation and Data Protection p.57
- 3.3 Rights and Obligations Under Applicable Data Regulation p.57
- 3.4 Regulators and Enforcement p.57

4. Sectoral Topics p.58

- 4.1 Use of Cookies p.58
- 4.2 Personalised Advertising and Other Online Marketing Practices p.58
- 4.3 Employment Privacy Law p.59
- 4.4 Data Protection in M&A p.60

5. International Considerations p.60

- 5.1 Restrictions on International Data Transfers p.60
- 5.2 Government Notifications and Approvals p.61
- 5.3 Data Localisation Requirements p.61
- 5.4 Blocking Statutes p.61
- 5.5 Recent Developments p.62

Zhong Lun Law Firm is one of the largest full-service law firms in China, with over 400 partners and more than 2,200 professionals, and offices in Beijing, Shanghai, Shenzhen and other major cities in China and around the world. The firm's cybersecurity and data protection team is an industry leader in China, with a wealth of experience in fields such as cybersecurity, data security and personal information protection. The partners are frequently invited to participate, as legal experts, in the legislative process relating to

cybersecurity and data protection legislation. Actively practising in the technology and telecommunications industries in the past two decades, and providing professional legal services to a large number of multinational clients that embrace the challenges of digitalisation, Zhong Lun has accumulated profound experience and developed a unique system of project compliance processes to assist in solving domestic and cross-border data protection issues.

Author



Jihong Chen is a senior equity partner at Zhong Lun and has been practising law and providing legal services for a large number of international enterprises since 1996. He specialises in cybersecurity, data

protection and privacy, telecoms law, IP and technology-related legal matters, and has been the Deputy Chairman of the IT/Hi-Tech Committee of the China National Bar Association since 2001. He has published widely in the areas of data protection, TMT, e-commerce and hi-tech law.

Zhong Lun Law Firm

22-24/F & 27-31/F
South Tower of CP Center
20 Jin He East Avenue
Chaoyang District
Beijing 100020
China

Tel: +86 010 5957 2003
Fax: +86 010 6568 1022
Email: chenjihong@zhonglun.com
Web: www.zhonglun.com



ZHONG LUN
中倫律師事務所

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Privacy and data protection provisions within the Chinese legal framework are scattered across laws and regulations at different legislative levels. In terms of specialised legislation on cybersecurity and data protection, China has established a comprehensive legal framework that includes several key laws and regulations – ie, the “Three Fundamental Laws”:

- the Cybersecurity Law (CSL; 网络安全法);
- the Data Security Law (DSL; 数据安全法); and
- the Personal Information Protection Law (PIPL; 个人信息保护法).

These operate together with the “Four Key Regulations”:

- the Regulations for the Administration of Network Data Security (RANDS; 网络安全数据管理条例);
- the Security Protection Regulations for Critical Information Infrastructure (关键信息基础设施安全保护条例);
- the Regulations on the Protection of Minors Online (未成年人网络保护条例); and
- the Regulations on the Graded Protection for Cybersecurity (Draft for Comments) (网络安全等级保护条例 (征求意见稿)).

The Three Fundamental Laws and the Four Key Regulations form the pillars of China’s cybersecurity and data protection legal framework, with each addressing different aspects of data security and privacy.

The CSL was enacted on 1 June 2017 and forms the backbone of cybersecurity and data privacy protection legislation in China. It underwent its first revision in 2025, which took effect on 1 January 2026, achieving co-ordinated integration with the DSL and the PIPL. The DSL came into effect on 1 September 2021 and is the fundamental law in the data security sphere, widely covering data security mechanisms, obligations and liabilities at both state administration and data handler level. The PIPL came into effect on 1 November 2021 and embraces the new era of personal information (PI) protection as well as corporate

data protection compliance. The Four Key Regulations further detail the cybersecurity and data protection requirements set forth in the Three Fundamental Laws from different perspectives.

In addition to the specialised legislation, China’s general legislation may also include provisions on privacy and data protection. Specifically, the Civil Code (民法典) plays a significant role in this regard. The Civil Code’s provisions relating to data privacy protections are basically consistent with the requirements provided in the Three Fundamental Laws, further solidifying the legal foundation for privacy and data protection in China. Data protection regulations on privacy are also scattered in:

- the Criminal Law (刑法);
- the Law on the Protection of Consumer Rights and Interests (Consumer Protection Law; 消费者权益保护法);
- the E-commerce Law (电子商务法); and
- Several Issues Concerning the Application of Law in the Trial of Civil Cases Relating to the Use of Facial Recognition Technologies to Process Personal Information (最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定), etc.

Extraterritorial Reach

The PIPL has an extraterritorial effect on overseas PI processing activities, when the processing is for the purpose of providing products or services to, or analysing individuals within, China. The extraterritorial application of the DSL will be triggered where data processing activities conducted outside the territory of China harm its national security, public interests, or the lawful rights and interests of its citizens or organisations. The newly amended CSL expands its extraterritorial application, stipulating that overseas organisations and individuals engaged in activities endangering China’s cybersecurity shall be held legally accountable, and, where serious consequences are caused, measures such as freezing assets or other necessary sanctions may be imposed.

Interplay With Other Laws Governing Non-Personal Data, Cyber and AI

The interplay between PI protection laws and other laws governing non-personal data, cyber and AI

in China is complex but complementary. The DSL establishes uniform baseline security management requirements for all types of data, including both personal and non-personal data. The CSL serves as the fundamental law for cyberspace governance and is designed to protect network operation security, network information security, and PI involved in network operations. With regard to AI-related laws, on one hand, the essential data protection laws (including the Three Fundamental Laws and the Four Key Regulations) are applicable to all data processing activities under AI-related scenarios. On the other hand, the AI-related laws specify and complement the data protection requirements in the context of AI.

Together, the PI protection laws and other laws governing non-personal data, cyber and AI provide a comprehensive approach to ensure cybersecurity and promote data and privacy protection. The above legal frameworks collectively address different aspects of data handling in China. However, they share unified objectives of enhancing cyber and data security and ensuring accountability in the digital age.

1.2 Rights and Obligations

General Principles and Requirements

The core principles for processing PI established by the PIPL include the following:

- legality, legitimacy, necessity and good faith;
- purpose limitation and data minimisation;
- transparency;
- data accuracy; and
- accountability.

Under these principles, the PIPL sets forth a series of specific compliance requirements, including obligations to notify data subjects, obtain appropriate legal bases, implement PI security safeguards and incident response measures, as well as to fulfil specific obligations regarding cross-border data transfer (CBDT).

Data Subjects' Rights

The PIPL provides PI subjects with the right, in relation to their data, to know, decide, restrict, refuse, access, copy, make portable, rectify, delete, and withdraw their consent. In addition, PI subjects are also provided with related rights on automated decision-making.

The right to data portability states that where PI subjects request to transfer their PI to another designated PI handler, such request shall be fulfilled by PI handlers when prescribed conditions are met.

Main Compliance Requirements for Organisations

To ensure compliance with the requirements of the PIPL, organisations should implement, at a minimum, the following compliance measures.

- Conduct data mapping due diligence of PI processing activities; identify whether the obligation to inform data subjects has been fulfilled and appropriate legal bases have been obtained. Identify CBDT scenarios and evaluate whether the corresponding obligations have been fulfilled.
- Carry out classified and graded management of PI.
- Establish internal management policies and operational procedures.
- Implement appropriate technical security measures.
- Formulate and implement emergency response plan. Take remedial action and make necessary reports in the event of a PI breach.
- Designate a PI protection officer to ensure the legal threshold is met.
- Conduct PI compliance audits.
- Perform a PI Protection Impact Assessment (PIPIA) prior to engaging in specific processing activities.

1.3 Special Categories of Personal Data

Under the PIPL, PI that is likely to result in damage to the personal dignity of any natural person or damage to their personal or property safety once disclosed or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts and tracks, as well as the PI of minors under the age of 14, is defined as sensitive PI.

Compared to general PI, sensitive PI is subject to more stringent protection requirements. It may be processed only for a specific purpose, where sufficiently necessary, and after strict protection measures have been taken.

According to Article 28 of the PIPL and the GB/T 45574-2025 Security Requirements for Sensitive Per-

sonal Information Processing (GB/T 45574-2025 敏感个人信息处理安全要求), the following constitute sensitive PI:

- health data;
- data about political/religious orientation;
- data on criminal convictions; and
- PI of minors under the age of 14.

The processing of such data requires the separate consent of the individual. In addition to the general notification items stipulated by the PIPL, the individual must also be informed of the necessity of processing the sensitive PI and its impact on their rights and interests. For processing the PI of minors under the age of 14, the consent of the minor's parents or other guardians must be obtained, and dedicated PI processing rules shall be formulated.

Regarding other special categories of PI, such as personal financial data and genetic data, their processing is governed by separate legislation or sector-specific laws and regulations.

1.4 Processing of Personal Data for Research and Development Purposes

Under the PIPL, “anonymisation” refers to the processing of PI in a manner that makes it impossible to identify certain natural persons and so that it cannot be recovered. Once data meets this standard, it is no longer considered PI, and its subsequent use generally does not require obtaining individual consent. However, achieving this status is contingent upon the company having fully fulfilled its obligation to inform and obtain the corresponding legal basis when processing the original data. In other words, the subsequent anonymisation process must be founded upon the lawful collection of the original data.

Furthermore, the Measures for Review of Scientific and Technological Ethics (Trial) (“Ethics Review Measures”, 科技伦理审查办法(试行)) stipulate that scientific and technological activities involving human participants, including those utilising human biological samples or PI, shall undergo a review of scientific and technological ethics. Entities engaged in scientific and technological activities in fields such as life sciences, where the research content involves areas sensitive to scien-

tific and technological ethics, shall establish a review committee for scientific and technological ethics.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Privacy Requirements for Use of Personal Data

AI-generated content (AIGC) developers and service providers should comply with essential data protection laws when carrying out PI processing activities. For instance, both the PIPL and the DSL require data minimisation and purpose limitation, which directly affects how AI models are trained. AI systems that process PI must ensure that users can exercise their rights as set out under the PIPL. AI systems must incorporate robust security measures to prevent breaches of PI and AIGC service providers shall build these features into their platforms to comply with such data protection requirements. Furthermore, Article 7 of the Interim Measures for the Administration of Generative Artificial Intelligence Services (“AIGC Measures”; 生成式人工智能服务管理暂行办法) provides that AIGC service providers shall ensure the lawfulness of the training model and data sources when processing training data, and data subjects' consent shall be obtained if any PI is involved.

Automated Decision-Making Using AI

Article 24 of the PIPL sets forth restrictions on the use of PI for automated decision-making. When utilising PI for automated decision-making through AI, the transparency of the decision-making process and the fairness and impartiality of the outcomes shall be ensured. Unreasonable differential treatment against individuals in terms of transaction conditions such as pricing is prohibited. When a decision significantly affecting an individual's rights and interests is made through automated decision-making, the individual is entitled to request an explanation and has the right to refuse the decision being made solely through automated decision-making.

Risk-Based Regime

China implements inclusive, prudent, categorised and tiered regulation over AIGC services, constituting a risk-based regime. There is no provision explicitly prohibiting the use of AI in specific high-risk application scenarios. However, AI shall not be used to generate illegal information or to engage in illegal activities. For

instance, it is prohibited to use AI to generate content that infringes upon the lawful rights and interests of others or endangers national security, etc. Furthermore, AIGC technology shall not be utilised to engage in monopolistic or unfair competition practices.

How AI Regulation Affects Data Protection in China

Where PI processing is involved in AI scenarios, the essential data protection laws shall be complied with. Simultaneously, specialised regulations governing AI, such as the AIGC Measures, impose further specific requirements regarding the PI processing in AIGC services. Specific provisions have been formulated in key data protection regulations to address AI development while simultaneously ensuring a balance between innovation and data protection. For instance, the newly amended CSL specifically incorporates framework provisions on AI safety and development, emphasising that China will improve ethical norms for AI and strengthen risk monitoring, assessment and security oversight.

The transparency requirements under the PIPL, which mandate the full fulfilment of notification obligations, are also applicable to AIGC services when processing PI. The AIGC Measures also require AIGC service providers to enhance the transparency of their services, as well as the accuracy and reliability of the generated content.

The RANDS provide that, in so far as the training data and processing activities thereof are concerned, the network data handlers providing AIGC services shall fulfil relevant security management obligations, which demonstrates the emphasis placed on data governance.

The Ethics Review Measures stipulate that entities engaged in AIGC activities, where the research content involves areas sensitive to scientific and technological ethics, shall establish an ethics review committee, conduct reviews of scientific and technological ethics for the AIGC activities and implement follow-up supervision over the AIGC activities.

1.6 Data Breach Requirement

According to Article 57 of the PIPL, in the event of a PI leak, alteration or loss, or where such an incident is likely to have occurred, the PI handler shall immediately take remedial measures and notify the competent authority and the affected individuals. The notification shall include:

- the categories of PI involved, the causes of the incident and the potential harm that may result;
- the remedial measures that have been taken and the measures individuals can adopt to mitigate the harm; and
- the contact details of the PI handler.

The Measures for the Administration of National Cybersecurity Incident Reporting (国家网络安全事件报告管理办法) further specify the thresholds, procedures and timelines for such reporting. For a “relatively major” incident – for instance, one involving the PI leakage of more than one million individuals – a report shall be submitted to the cyberspace administration authority within four hours. If the network operator is a Critical Information Infrastructure Operator (CIIO), the report shall be submitted within one hour.

Upon being informed of the incident, the competent authority may initiate an investigation in accordance with the law. Mass data privacy litigation is also possible – refer to **2.3 Collective Redress Mechanisms** for more details.

1.7 Regulators

Key Regulators and Their Core Competence

Since data regulation is a topic that impinges upon all industries, there is a wide range of law enforcement departments related to it, many of which have intersecting duties and authorities. There is no centralised regulatory body. Among all these regulators, the most important ones include:

- the Cyberspace Administration of China (CAC);
- the Ministry of Public Security (MPS); and
- the Ministry of Industry and Information Technology (MIIT).

The CAC is in charge of overall planning with regard to data protection and privacy, and co-ordinates the

competent authorities. The MIIT, the MPS, the State Administration for Market Regulation (SAMR) and other industry regulators are in charge of law enforcement in the respective industries.

Typical Investigative Workflow

Investigations initiated by regulators can be triggered in different ways, including:

- reporting – where users may report to the regulators and consumer protection organisations, and investigations are launched accordingly;
- regular and irregular inspections – where special projects that last several months are launched to target specific industries or pain points in cyberspace; and
- inquiries into data leakage events, network loopholes or other cybersecurity/data incidents.

While conducting investigations, special rules shall be followed by the regulators. For instance, the Measures for Supervision and Inspection of Cyberspace Security by Public Security Organs (Draft for Comments) (公安机关网络空间安全监督检查办法(征求意见稿)) prescribes the procedures for law enforcement inspections conducted by public security organs. The Provisions on Administrative Law Enforcement Procedures of Cyberspace Administration Departments (网信部门行政执法程序规定) set the rules to oversee the investigations initiated by the CAC. The MIIT must conduct its enforcement activities in accordance with the List of Administrative Law Enforcement Matters of the Ministry of Industry and Information Technology (2025 Edition) (工业和信息化部行政执法事项清单(2025年版)).

Domestic and Cross-Border Co-Ordination Mechanism

The CAC is in charge of overall planning with regard to data protection and privacy, and co-ordinates the competent authorities. A collaborative mechanism has been established among various departments for information sharing and case transfer. For instance, if the CAC or the industrial authority discovers any clues indicating criminal offences, they will transfer the case to the public security organs. There is no Chinese equivalent to GDPR “lead supervisory authority” mutual-recognition.

Binding Force of Guidance

In China, regulatory documents in various forms possess a hierarchical binding effect, collectively shaping the compliance framework for enterprises. Documents issued in the form of departmental rules carry legal enforceability. Violations of such rules may directly result in administrative penalties. Guidance documents – such as policy interpretations, FAQs, and typical case studies issued by authorities – do not in themselves create direct binding legal force. However, they articulate the official interpretation and prevailing enforcement priorities of the regulators, serving as critical reference materials for corporate compliance.

1.8 Enforcement Proceedings and Fines Investigations and Enforcement Actions

When initiating administrative proceedings and enforcing the laws, the competent authorities must abide by the Law on Administrative Penalty (行政处罚法). The competent authorities should conduct investigations to ascertain the facts of the alleged violating acts before imposing punishment on anyone (Article 54). For triggers of investigations, refer to 1.7 Regulators.

Regulators shall promptly notify the parties concerned of the facts of the violation and facilitate their submission of statements and defences (Article 41). Generally, the regulator shall make the administrative penalty decision within 90 days from the date of case filing (Article 60). Prior to rendering an administrative penalty decision, the regulator shall inform the parties of the proposed penalty and its legal basis (Article 44).

The penalised parties are entitled to a hearing in cases where the administrative penalty involves the suspension of business, rescission of a business permit or licence, or a large penalty (Article 63). If a party is dissatisfied with an administrative penalty, it has the right to apply for administrative reconsideration or file an administrative lawsuit (Article 7).

Sanctions and Remedies

The Three Fundamental Laws uniformly stipulate that any violation of the laws which causes damage to others shall bear civil liability. Where a crime is constituted, criminal liability shall be imposed.

For administrative penalties, under the PIPL, the penalties for violations may include:

- an order of rectification;
- warning;
- confiscation of illegal earnings; or
- the suspension or termination of apps or services.

For severe violations, the violator may be fined up to CNY50 million or 5% of its turnover of the previous year at the company level, and the person directly in charge will be fined up to CNY1 million. The company's business licences and permits may also be revoked.

Depending on the nature and severity of the violation, different sanctions and penalties may be imposed by the CSL. Authorities may:

- order rectification;
- issue warnings;
- impose fines on both the enterprise and the directly liable person(s); and
- (where the circumstances are serious) suspend the offending business line, order suspension-for-rectification, or revoke the relevant business licence or the company's business licence.

The amended CSL materially raises the ceiling for administrative fine to CNY10 million, thereby aligning it with the upper limit already provided in the DSL.

The authorities will determine the amount of any fine on a case-by-case basis, taking into consideration the severity of the violating acts, infringements of legitimate rights and interests on individuals, any adverse impact on society, etc. The administrative authorities may, in accordance with law, formulate discretion benchmarks for administrative penalties to regulate the exercise of such discretion. Such discretion benchmarks shall be made public.

Under Article 33 of the Law on Administrative Penalty, no administrative penalty shall be imposed under the following circumstances:

- where the illegal act is of a minor nature, has been timely rectified, and has caused no harmful consequences;
- where the act constitutes a first-time violation, the harmful consequences are minor, and it has been timely rectified; or
- where the party concerned provides sufficient evidence to prove the absence of subjective fault.

1.9 Enforcement Trends

Significant data enforcement actions and trends in the past 24 months include the following.

- In 2024, the MPS launched the "Clean Network" (净网) operation, investigating and resolving over 7,000 cases involving PI infringement.
- In March 2025, the CAC, MIIT, MPS and SAMR jointly issued an announcement on the launch of the 2025 Special Campaign Series for Personal Information Protection.
- In 2025, the MPS initiated the "Protecting Networks 2025" (护网2025) special operation, focusing on penalising failures to fulfil obligations related to cybersecurity, data security and PI protection.
- From April to July 2025, the CAC carried out the "Clear and Bright: AI Technology Abuse Rectification" (清明·AI 技术滥用整治) campaign, shutting down unregistered LLM applications, investigating training data from illegal sources, and cracking down on the use of AI to create illegal content.
- The MIIT regularly publicly announces and orders the removal of apps that infringe upon users' rights and interests.

The practical takeaways for organisations are as follows.

- Conduct regular self-audits and risk assessments, integrate compliance reviews into the development and launch processes for new products and services.
- Actively monitor the official notices, typical cases and enforcement trends published by regulatory authorities.
- Focus on areas subject to frequent regulatory penalties. In accordance with the key compliance issues highlighted in notices from authorities, conduct self-inspections to determine whether the

organisation's apps engage in practices such as unauthorised PI collection, excessive permission requests, etc.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Over the past 24 months, privacy and data-related disputes adjudicated by Chinese courts have exhibited a notable trend characterised by a surge in case numbers and a refinement of adjudication rules. First, there has been a marked increase in the number of data-related cases heard by the courts. According to announcements by the Beijing Internet Court, it received a total of 113 cases related to PI protection disputes between October 2023 and October 2024. In contrast, merely 58 such cases were handled by the same court in the past five years leading up to 2023. Secondly, adjudication rules are becoming more unified and clearer: to address difficulties in judicial practice, the Supreme People's Court, in August 2025, issued for the first time a series of guiding cases on the judicial protection of data rights and interests, establishing uniform adjudication standards for core issues such as data ownership and PI protection.

Claimant Types and Common Causes of Action

In China, the majority of PI protection litigation cases are public interest litigation brought by procuratorial organs and consumer organisations. China also allows individuals to initiate private litigation, and the legal bases for an individual to initiate private litigation mainly include the Civil Code, the Consumer Protection Law, the CSL and the PIPL. Common causes of action include:

- collecting, disclosing or providing PI without consent;
- excessive PI collection;
- PI leakage; and
- exercising PI rights, etc.

Typical Remedies and Non-Material Damage

Typical remedies for privacy disputes include:

- cessation of infringement;
- apologies; and

- compensation for damages.

Regarding non-material damage, Article 1183 of the Civil Code stipulates that where an infringement upon an individual's personal rights and interests causes serious mental damage, the infringed party has the right to claim compensation for mental damages. Observing cases of typical PI disputes, published by the courts, in some instances courts have supported compensation for mental damage. The prerequisite for supporting such a claim is that the infringement upon PI-related rights has resulted in serious mental distress, which must exceed the tolerance limit of an ordinary person. The amount of compensation should correspond to the severity of the mental distress and is determined flexibly by the courts based on the specific circumstances of each case.

2.2 Recent Case Law

In August 2025, the Supreme People's Court released guiding cases on the judicial protection of data rights and interests, addressing issues of high public concern such as the determination of data ownership and PI protection, thereby unifying the adjudication standards for similar cases.

In one case where an individual sued an app for excessively collecting users' PI, the app required the submission of user profile information such as educational stage and English proficiency level, without providing options such as "skip" or "refuse", nor offering alternative login methods for users who disagreed with providing such information. The court held that user profile information did not constitute necessary PI for the app to provide its basic functional services. Therefore, the legal basis of "necessary for contract conclusion or performance" was not applicable, and consent should have been obtained. The app's design forced users to check the "agree" box for using the app. Such "consent" was given involuntarily and thus did not constitute valid consent.

2.3 Collective Redress Mechanisms

Article 70 of the PIPL establishes the mechanism of public interest litigation for PI infringement. Where any PI handler illegally processes PI, which infringes upon the rights and interests of a large number of individuals, a lawsuit may be brought to the court by:

- the People's Procuratorate;
- the consumer organisations specified by law; and
- the organisations determined by the CAC.

In the past few years, the number of public interest litigation cases regarding PI protection has increased year by year. From July 2015 to September 2025, prosecutors have handled nearly 25,000 cases specifically focused on PI protection. This upward trend reflects the growing frequency of legal actions concerning PI protection initiated by prosecutors and shows the great importance attached to PI protection.

The core admissibility criteria is that the illegal PI processing must infringe upon the rights and interests of a large number of individuals, thereby harming the public interest. As stipulated in the Draft Procuratorial Public Interest Litigation Law (检察公益诉讼法(草案)) released on 28 October 2025, the admissibility of such litigation is also contingent upon preliminary evidence indicating the commission of an unlawful act.

Concerning indicative timelines, after a procuratorate places a case on file, it must decide whether to initiate civil public interest litigation within one year. For cases that are major, complex or difficult, this period may be extended. Subsequent litigation stages, including trial and appeal, are generally subject to the time limits prescribed by the Civil Procedure Law (民事诉讼法).

In terms of relief, a court may order the defendant to cease the infringement and assume liabilities such as:

- eliminating the adverse effects;
- restoring reputation;
- making apology; and
- providing compensation.

Furthermore, under the court's auspices, the procuratorate may reach a mediation agreement or a settlement with the defendant regarding the enforcement of the judgment.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

With regard to non-personal data protection, China has established a fundamental legal framework centred on the DSL. Furthermore, the Three Fundamental Laws operate synergistically to cover the entire life cycle of data processing. The RANDS, which apply to all network data processing, mark a co-ordinated regulatory framework that unifies privacy, data security and non-personal data governance under shared obligations.

Regarding cross-sector data access and sharing frameworks for IoT, cloud computing or other data processing services, China has not enacted unified legislation for their regulation. Instead, such frameworks are predominantly governed by a combination of data protection laws, sectoral regulations and industry-specific guidelines – ie, the Three Fundamental Laws, as well as certain industrial measures and/or standards such as:

- the Measures on Safety Evaluation for Cloud Computing Services (云计算服务安全评估办法); and
- Information Security Technology – Security Technical Requirements of Data Transmission for IoT (GB/T 37025-2018 信息安全技术 – 物联网数据传输安全技术要求), etc.

China also promotes the secure use and free flow of such data, promotes the availability and accessibility of data and enhances the activity of the data-driven economy, as set out under the Opinions on Building a Basic Data System to Better Play the Role of Data Elements (“Opinions”; 关于构建数据基础制度更好发挥数据要素作用的意见).

Under China's legal framework, all entities processing data – whether as IoT service providers (similar to data holders) or as parties that obtain and process data through transactions, licensing or other means (similar to data users) – are subject to statutory obligations for data processing. The PIPL and the DSL delineate distinct rights and responsibilities for different roles, notably data handlers (comparable to data controllers under the GDPR) and entrusted parties

of data processing (comparable to data processors under the GDPR). In addition, the Opinions establish protections for data originators from the perspective of data ownership.

The frameworks encompass both personal and non-personal data. The DSL adopts a broad definition of data, which includes any information recorded in electronic or non-electronic form. Consequently, non-personal data, such as industrial data, also falls within the scope of protection under the DSL. The protection of PI is primarily governed by the PIPL.

Currently, China has not enacted a single, standalone law equivalent to the Data Act. Instead, it has adopted a model that combines comprehensive legislation with supporting policies. Foundational laws establish the framework for safeguarding data sovereignty and security, while policies like the Opinions are progressively advancing the marketisation of data. This approach aims to strike a prudent balance between promoting data sharing and innovation on one hand, and addressing security concerns on the other.

3.2 Interaction of Data Regulation and Data Protection

The interaction between the above data regulation frameworks and privacy rules, as well as the IP protection of non-personal data, is not realised through a single statutory provision, but accomplished through a layered, multi-dimensional and dynamically evolving comprehensive legal system. The core logic resides in the foundational legal framework constituted by the Three Fundamental Laws, which establish red lines and principled obligations for all data processing activities.

Specifically concerning PI processing, data generated by IoT or cloud computing services, once constituting PI, must fully comply with PI processing obligations stipulated under the PIPL. This includes ensuring a legal basis as defined by the PIPL, such as obtaining user consent. Concurrently, regulations pertaining to IoT or cloud computing require service providers to implement technical measures – such as encryption and access control. These requirements constitute the operational implementation of the overarching legal principles of “confidentiality” and “security”.

Non-personal data generated by the IoT or processed via cloud computing – such as industrial data – is regulated by the DSL and CSL in terms of its storage, transmission and cross-border security. While raw IoT data, such as sensor readings, generally does not constitute intellectual property (IP) in itself, once such data undergoes original compilation or in-depth analysis, it may give rise to a data product eligible for copyright protection or protectable as a trade secret, thus falling within the scope of IP law.

3.3 Rights and Obligations Under Applicable Data Regulation

The processing of PI within contexts such as the IoT and cloud computing is likewise subject to the Three Fundamental Laws, encompassing the stipulated rights and obligations as well as the necessary action items for organisations. For details, refer to **1.2 Rights and Obligations**.

For non-personal data, the DSL seeks to safeguard the rights of data owners by imposing obligations on data processing. Organisations are required to establish a data management system and implement technical measures to ensure data security. In terms of data circulation, China encourages the compliant and efficient use of data, while establishing security boundaries for data sharing and trading. For instance, data intermediary service providers are obligated to verify the legality of data sources and the identities of the parties involved in data transactions.

3.4 Regulators and Enforcement

Pursuant to the DSL, China has established a co-ordinated working mechanism for data security, applicable to data including non-personal data. Local authorities and various government departments are responsible for the data collected and generated within their respective regions and sectors, as well as for the security of such data. The CAC takes the lead in co-ordinating network data security efforts and related regulatory work. The MPS and other relevant authorities undertake data security regulatory responsibilities within their respective statutory remits. Sector-specific authorities, such as the MIIT and those overseeing transportation, and finance, assume data security regulatory duties for their respective industries.

Moreover, the National Data Bureau, inaugurated in October 2023, is responsible for overseeing the integration, sharing and development of data resources, co-ordinating the construction of data infrastructure systems, and the planning and construction of digital China, the digital economy and digital society.

Co-Ordination With Privacy and Competition Authorities

The regulation of PI and non-personal data is integrated through a shared enforcement framework. The CAC leads the enforcement of the PIPL but its mandate extends into network data issues, which may involve non-personal data regulation. Sectoral authorities also assume regulatory duties over both PI and non-personal data within their respective industries.

China's competition authorities, primarily the SAMR, also collaborate with non-personal data regulators. In early 2025, the SAMR, jointly with the National Data Bureau, the CAC and three other departments, issued the Implementation Plan for Improving the Security Governance of Data Circulation to Better Promote the Marketization and Value Realization of Data as a Factor of Production ("Implementation Plan", 关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案). It explicitly stipulates the punishment of monopolistic and unfair competition practices involving the use of data, thereby providing guidance for subsequent enforcement by the SAMR. In daily operations, these authorities have established mechanisms for information sharing, case notification, and co-ordinated law enforcement. For instance, non-personal data regulators may transfer leads to the SAMR if they discover indications of unfair competition involving data during routine oversight. Conversely, when investigating cases of data-related unfair competition, the SAMR may require the CAC to provide professional input on data regulation.

Enforcement Trends

The joint formulation and issuance of core policies by multiple authorities has become a regular practice. A case in point is the Implementation Plan, which aims to promote the utilisation of data. Various sectoral authorities have intensively introduced detailed data rules specific to their respective industries. For example, both the People's Bank of China and the MIIT

have issued or drafted relevant sector-specific regulations, thereby making the oversight more scenario-specific and practical.

4. Sectoral Topics

4.1 Use of Cookies

The use of online tracking technologies is usually regarded as PI collection, which must comply with PI protection-related requirements. According to the PIPL, the collection and use of PI must follow the principles of legality, legitimacy and necessity, which means that the use of online tracking technologies for user information collection must comply with these principles. Individuals must be truly, accurately and completely informed in a prominent manner and in clear and understandable language, and consent must be obtained. The "opt-out" model is generally not permitted under the core principles of the PIPL.

4.2 Personalised Advertising and Other Online Marketing Practices

The Advertising Law (广告法) is the fundamental law that regulates advertising. The Measures for Administration of Internet Advertising (互联网广告管理办法) apply to online marketing. The sender must obtain consent to, or a request for, advertising from the recipients, and the sender must also disclose their true identity, contact details and the opt-out method for advertisements distributed via electronic means.

Restrictions on Profiling

Pursuant to Article 24 of the PIPL, if business marketing or push-based information delivery is conducted towards an individual by means of automated decision-making, an option not targeting the personal characteristics of the individual, or an easy way to refuse to receive this, must be provided to the individual. In addition, according to the Information security technology – Personal information security specification (GB/T 35273–2020 信息安全技术 个人信息安全规范), the use of indirect user profiling generated from PI that is not from particular persons is recommended for online marketing, rather than direct user profiling.

Restrictions on Use of Sensitive or Children's Data for Marketing Purposes

The collection and use of sensitive PI for marketing purposes is subject to strict limitations under the PIPL. For any marketing activity involving sensitive PI, separate consent must be obtained, and individuals shall be informed of the necessity of processing sensitive PI and the impact on their rights.

Regarding children's data, which is classified as sensitive PI under the PIPL, enhanced protections are established. When processing the PI of minors under the age of 14, the consent of their parents or other guardians must be obtained. The Regulations on the Protection of Minors in Cyberspace (未成年人网络保护条例) stipulate that commercial marketing shall not be conducted towards minors through automated decision-making methods. Consequently, the use of children's data for marketing purposes may only proceed under these strictly limited conditions.

Consent Requirements

Since online marketing, particularly personalised advertising, is normally based on the analysis of PI collected from users, regulations on PI collection and use must be observed. PI may not be collected or used for personalised advertising if the PI subjects have not agreed to this.

4.3 Employment Privacy Law

The PI processing requirements stipulated in the Three Fundamental Laws are also applicable to the employment context. As an exception, where the processing of employee PI is necessary for human resources (HR) management purposes, consent or applying the CBDT mechanisms (refer to 5.1 Restrictions on International Data Transfers for details) may no longer be required. However, it is essential to ensure that any such processing is conducted in accordance with lawfully established labour rules or legally executed collective contracts. Additionally, the HR necessity of the data processing must be clearly substantiated.

Employees Monitoring

The monitoring of employees, such as through time-tracking systems, must comply with principles of necessity and legitimacy. Employers should inform employees of the monitoring purpose, scope and

methods. Processing must be justified as necessary for HR management (eg, performance assessment) under lawful labour rules; otherwise, consent must be obtained.

Remote Work

For remote work, employers must establish clear policies regarding the use of company-provided or personal devices. Employees should be informed about data collection related to remote activities (eg, work hour logs), and the data processing must adhere to the "necessity" test under labour rules.

Use of IT Systems

Employers using IT systems (eg, email, internal platforms) to process employee data must define the purpose and scope in labour rules or labour contracts. Processing for HR management (eg, payroll, attendance) typically does not require consent. However, for systems involving non-essential data for HR management, consent may be needed.

Bring Your Own Device Policies

BYOD policies require balancing security needs with employee privacy. Employers must clarify employee PI collection scope in the BYOD scenario and implement security measures for the collected data accordingly. Consent may be needed if processing extends beyond HR necessities.

Background Checks

Background checks must be lawful, necessary and transparent. Employers should obtain prior consent and limit checks to job-relevant information. Excessive data collection, such as unrelated health details, is not allowed. Results must be kept confidential and securely stored, with retention periods aligned with HR purposes.

Job Application

For job applications, employers must inform candidates of the data processing purposes, such as recruitment evaluation. Consent is typically required, and separate consent may be needed as stipulated in the PIPL. Data of unsuccessful applicants should be deleted after the necessary retention period expires, in accordance with the data minimisation principle.

4.4 Data Protection in M&A

All forms of data processing activities occurring in M&A and asset deals shall be governed by the DSL and the PIPL. The requirements and obligations set forth under the DSL and the PIPL shall be complied with accordingly.

Due Diligence Phase

Acquiring parties must adhere to the principle of data minimisation and necessity. Access to and review of the target company's PI should be limited to what is strictly essential for the due diligence. Robust confidentiality agreements must govern all parties to prevent unauthorised use or disclosure of PI.

Notification Upon Change of Control

With regard to any transfer of PI due to change of control, Article 22 of the PIPL specifies additional disclosure requirements that relevant individuals shall be informed of the name and contact information of the PI recipient. Individual's consent is not required.

Post-Closing Integration

The PI recipient (the acquirer) must ensure its subsequent processing complies with the original purpose and method as understood by the individuals. In the event of any changes to the original purpose and method of data processing, consent shall be re-obtained.

within China, but can be queried, accessed, downloaded or exported remotely from overseas. It should be noted that if activities involving the PI processing of individuals within China are conducted outside China, with the purpose of providing products or services to such individuals or analysing or evaluating their behaviour, this also constitutes CBDT.

To lawfully conduct CBDT, data handlers must select and fulfil a specific compliance pathway based on the nature and the volume of data transferred. There are three main CBDT compliance routes:

- obtaining the CAC security assessment approval, a mandatory prior approval required from the CAC, applying to –
 - (a) CIIOs transferring PI or important data abroad; and
 - (b) non-CIIO data handlers transferring important data, or transferring, since January 1 of the current year, PI of more than 1 million individuals or sensitive PI of more than 10,000 individuals;
- being certified by the recognised agencies ("Certification"); or
- concluding the CAC's prescribed standard contractual clauses with the overseas recipient and filing it with the provincial CAC within 10 working days of its effectiveness (SCCs).

For non-CIIO data handlers whose cumulative transfers since January 1 fall within the range of 100,000 to 1 million individuals' PI, or less than 10,000 individuals' sensitive PI, and do not involve important data, the Certification and SCCs routes are alternative options – the data handler may choose either one.

Crucially, onward transfers by the overseas recipient are subject to strict regulation and must meet several conditions. These include, but are not limited to:

- providing comprehensive notice to the individual;
- obtaining separate consent; and
- executing a binding agreement with the onward recipient.

5. International Considerations

5.1 Restrictions on International Data Transfers

According to China's regulatory framework, the CBDT of data encompasses both PI and non-personal data, the latter primarily referring to "important data" – the data that, once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger national security, economic operation, social stability, public health and security, etc.

A "transfer" or "outbound transfer" is broadly construed as a data handler transferring data, collected and generated during its operations within China, to locations outside China. It also includes situations where the data collected and generated is stored

This agreement must ensure that the recipient's PI processing complies with the protection standards stipulated by Chinese laws.

Regarding exceptions, Article 38 of the PIPL allows the provision of PI according to international treaties or agreements concluded or acceded to by China. Furthermore, Provisions on Promoting and Regulating Cross-Border Data Flows ("CBDT Provisions", 促进和规范数据跨境流动规定) provide for the following scenarios that are exempt from the CBDT application procedures:

- CBDT that does not contain PI or important data;
- where data handlers transfer PI collected and generated overseas after being processed domestically without involving domestic PI or important data in the process;
- for the establishment or performance of contracts to which individuals are parties;
- in implementing cross-border HR management based on legally formulated labour rules and collective contracts;
- in emergency situations to protect the life, health and property safety of natural persons; and
- where a non-CIIO data handler provides PI of fewer than 100,000 individuals (excluding sensitive PI) to an overseas recipient since January 1 of the same year.

Further, according to Article 6 of the CBDT Provisions, Free Trade Pilot Zones (FTZs) may formulate their own lists of data that is applicable to the CBDT mechanism (Negative List). Data handlers within the FTZs are exempted from applying the CBDT mechanism when providing data not included on the Negative List overseas.

5.2 Government Notifications and Approvals

For transferring PI and important data abroad, refer to 5.1 Restrictions on International Data Transfers.

In addition, the CBDT of certain specially regulated data (eg, human genetic resources information) is subject to specific regulatory rules provided in certain fields and may require government approval, according to applicable regulatory rules for such CBDT.

5.3 Data Localisation Requirements

In China, the first and foremost data localisation requirement is that national secrets are not allowed to be transferred overseas. Secondly, PI and important data collected by CIIOs in the course of their operations in China are required to be stored domestically, and a security assessment is required for CBDT.

There are also localisation requirements for specially regulated business data, including relating to the following:

- credit information;
- personal financial information;
- map data;
- essential tech equipment required for online publication services;
- data and information related to car hailing services;
- health information of the population; and
- insurance data and fiscal data.

In principle, such data must be stored within China (excluding the Hong Kong, Macau and Taiwan regions) and may not be freely transferred overseas.

Regarding remote access, accessing data stored in China from overseas typically constitutes a data transfer. Consequently, any such data transfer or remote access will be subject to the specific CBDT requirements applicable to the respective data type.

5.4 Blocking Statutes

The Rules on Counteracting Unjustified Extra-Territorial Application of Foreign Legislation and Other Measures of the People's Republic of China ("the Rules"; 阻断外国法律与措施不当域外适用办法) released by the Ministry of Commerce are considered to be China's blocking statute and have set up a relatively comprehensive anti-economic sanctions system to deal with the long-arm jurisdictions of certain countries and regions.

The Rules and the privacy laws work together – often complementarily – to create a comprehensive framework that limits foreign-driven data access or discovery from within China. The Rules addresses foreign regulatory orders broadly (not limited to PI), while the DSL/PIPL focus on data sovereignty, PI protection and data transfers. According to Article 36 of the DSL,

organisations may not provide any foreign judicial or law enforcement body with any data stored within China without the approval of the competent authority.

5.5 Recent Developments

Key Recent Developments

Measures for the Certification of Cross-Border Provision of Personal Information, which came into force on 1 January 2026, signify the comprehensive implementation of China's CBDT compliance framework. Serving as the final and integral component of the CBDT mechanisms, these Measures provide companies with a clear and stable compliance pathway through a market-based certification mechanism, thereby refining the overarching CBDT regulatory framework.

In September 2025, the National Cybersecurity Notification Center publicly disclosed an enforcement case in which a multinational enterprise was penalised for illegal CBDT activities. The identified violations included failure to do the following:

- complete the requisite security assessment for the CBDT;
- provide adequate notification to its users regarding the transfer;
- obtain separate consent from users; and
- implement necessary security technical measures.

Expected Future Developments in 2026

In 2026, the CBDT Certification mechanism will likely become another compliance route for companies. Companies need to prepare for this shift by ensuring their data protection practices align with the certification criteria.

It is anticipated that the formulation and implementation of the Negative List within FTZs will be significantly accelerated in 2026. Practical enforcement at the local level is already underway, with numerous FTZs having released Negative Lists in 2024 and 2025. Driven by central policy guidance and solidified through successful local pilots, 2026 is expected to be a pivotal year during which more FTZs will advance the development and implementation of their respective Negative Lists.

Trends and Developments

Contributed by:

Vincent Wang, Xinyao Zhao and Alfred Feng
Global Law Office

Global Law Office (GLO) dates back to the establishment of the Legal Consultant Office of China Council for the Promotion of International Trade in 1979. After more than 40 years of persistent effort and development, it has become one of the most prominent large comprehensive law firms in the Chinese legal industry. GLO has been committed to the mission of “serving domestic and foreign clients with globalised vision, a globalised team and globalised quality” since

its inception, enabling it to maintain a leading position in the industry in an ever-changing global economic environment. All lawyers at GLO are graduates from first-tier domestic and/or international law schools, most of whom hold LL.Ms or higher degrees. Many partners are qualified to practise law in the US, UK, Australia, Switzerland, New Zealand or Hong Kong, among others.

Authors



Vincent Wang is a partner at Global Law Office, based in the Shanghai office. With a focus on multinational business and cross-border transactions, he has particular expertise in navigating novel and

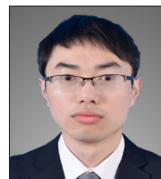
complex legal challenges in the TMT sector. Examples of the wide range of industries Vincent covers include telecommunications, e-commerce, cybersecurity and data protection, fintech business, electronic payments, internet-related businesses, high technology manufacture and engineering, new and emerging technologies (such as AI, blockchain, cryptocurrency, IoT, e-mobility, cloud computing, etc), e-automotive, medical devices, new media and streaming entertainment, food and beverage, agriculture and farming, and cross-border trade and investment.



Xinyao Zhao is a partner at Global Law Office, based in the Shanghai office since joining in 2018. Her main practice areas include cyber and data security, personal information protection, and corporate regulatory

compliance. She specialises in advising both multinational and domestic companies in areas

including telecoms, internet-related industries, IoT, automotive, e-commerce, fintech and healthcare. Xinyao has advised well-known international companies in completing their data compliance projects, providing support throughout the implementation process. Additionally, she has assisted domestic companies with their overseas business development in the USA, Europe and South-East Asia, focusing on data privacy compliance.



Alfred Feng is an associate at Global Law Office, based in the Shanghai office. Prior to joining Global in 2025, he worked for a branch office of a China law firm in Shanghai. His main practice areas include personal

information protection and data compliance, corporate compliance and dispute resolution. Alfred has assisted clients with due diligence review, contract drafting, review and negotiation, advising on the management and design of clients' apps/mini-programs, and providing opinion on the filing of cross-border data transfer and other specific legal issues. He has provided these legal services to many multinational companies in the fields of retail, medical health and industrial manufacturing.

Global Law Office

36th Floor, Shanghai One ICC
999 Middle Huaihai Road
Xuhui District
Shanghai 200031
China

Tel: +86 21 2310 8288
Fax: +86 21 2310 8299
Email: vincentwang@glo.com.cn
Web: www.glo.com.cn



环球律师事务所
GLOBAL LAW OFFICE

SINCE 1979

Data Practice in China in 2025: A Year-End Review

2025 saw noteworthy developments in cross-border data transfer, personal information compliance audit and artificial intelligence (AI), including rules for the certification of cross-border provision of personal information, revision of the Cybersecurity Law, and detailed requirements on AI-generated contents. All these efforts highlight China's desire to establish a secure and dynamic digital economy that addresses domestic growth needs while keeping an eye on global digital trade.

Note that the term data processors, as used in this chapter of the guide, is interchangeable with data controllers as defined by the GDPR, as that term is defined by the Personal Information Protection Law of the PRC (PIPL). Data processors, as defined by the GDPR, are referred to as contracted processors in this chapter.

New rules on cybersecurity and data protection

Revision of the Cybersecurity Law

The Cybersecurity Law of the PRC was revised in 2025 and took effect on 1 January 2026. The revised version explicitly specified that China is willing to support basic theoretical research on AI and research and development of key technologies such as algorithms, which signals that the Chinese government deems emerging technologies and their development activities as critical elements of cybersecurity. In addition, the new Cybersecurity Law significantly increased the face value of penalties for violating companies and responsible individuals, up to CNY10 million for severe compliance issues.

Measures for the Administration of National Cybersecurity Incident Reporting

The Measures for the Administration of National Cybersecurity Incident Reporting (the "Measures for Incident Reporting") were released by the Cyberspace Administration of China (CAC) on 11 September 2025 and came into effect on 1 November 2025. This regulatory instrument makes provision regarding when and how network operators shall report to the relevant authority in case of a cybersecurity incident.

Highlights of the Measures for Incident Reporting are as follows:

- define standards to determine the severity of cybersecurity incidents, including the duration of impact, the number of people that are involved, the amount of data leaked due to such incidents, and the damage caused by such incidents, etc;
- set a clear severity-based time limit for the network operators to report incidents to the authority;
- clarify items that should be reported to the authority; and
- announce the official channel for receipt of security incidents reports.

Following the release of the Measures for Incident Reporting, network operators should accordingly update their contingency plans for responding to security incidents in order to ensure compliance with the new regulation.

Determination of sensitive personal information

Sensitive personal information is subject to stricter protection under the law, but the definition and list

of sensitive personal information has become a soap drama in practice.

Article 28 of the PIPL defines it as personal information that is likely to result in damage to the personal dignity of any natural person or damage to their personal or property safety once disclosed or illegally used. As this definition is vague, in practice, most data processors will use the list of examples of sensitive personal information in Annex B of the national standard “Information security technology – personal information security specification” (GB/T 35273-2020, the “Information Security Specification”) as a key reference in determining sensitive personal information.

Though the Information Security Specification is only a recommended standard that showcases the recommended best practice, Chinese authorities explicitly use it anyway to determine sensitive personal information for law enforcement purposes. A good example of such a practice is the sensitive personal information defined in the official standard contract template for cross-border personal information transfer.

In 2025, a new national standard related to the determination of sensitive personal information was released, namely the Data security technology – Security requirements for processing of sensitive personal information (GB/T 45574-2025, the “Security Requirements for Sensitive Personal Information”). It not only provides a new list of sensitive personal information but also includes a new standard to determine sensitive personal information that is theoretically understandable for perfection but difficult to implement in practice. According to such a standard, if several types of non-sensitive personal information can be collectively used to cause an impact on personal dignity, personal safety or property safety, such a combination of non-sensitive personal information should also be considered as sensitive personal information.

Therefore, according to the Security Requirements for Sensitive Personal Information, data processors cannot only rely on a standard list to determine the sensitivity of personal information, but should consider the after-the-fact use and resulting impacts of the use of the non-sensitive personal information to determine whether such non-sensitive personal infor-

mation should be otherwise re-determined as sensitive personal information.

Apparently, it is a subjective standard – but it does not explain to whose mind it should be subject. Determination of sensitive personal information remains a puzzle, a more difficult one to solve, unfortunately.

Personal information protection compliance audit

The Personal Information Protection Compliance Audit is a requirement under the PIPL since 2021. The long-awaited practical rules to fulfil the audit requirement were released in the Administrative Measures on Personal Information Protection Compliance Audit (the “PIPCA Measures”) on 12 February 2025, which came into effect on 1 May 2025. The PIPCA Measures provide (in the annex) that the audit should cover 26 key areas, which virtually covers all compliance aspects regarding personal information processing.

The good news is that the PIPCA Measures only require that data processors processing personal information of over 10 million individuals must conduct a PIPCA at least every two years, either on their own or by an authorised external professional institution. There is no set time and frequency for other data processors to complete it so far, at least in the literacy of the law.

However, in certain areas, time limits may be imposed on data processors. For example, on 29 December 2025, the CAC released the Announcement on the Submission of Compliance Audit Results for the Protection of Personal Information of Minors (the “Announcement”). The Announcement requires all data processors that process personal information of minors under the age of 18 to conduct audits regarding minors’ personal information processing, and the result of the audit should be uploaded to CAC’s official website before 31 January 2026. Such short notice makes compliance with this unexpected requirement a serious challenge for all data processors that process personal information of minors.

Supervision of facial recognition technology

In 2025, facial recognition technology was a focus of the Chinese authorities. The Administrative Measures on the Application Security of Facial Recogni-

tion Technology (the “Measures on Facial Recognition Technology”) were jointly released by the CAC and the Ministry of Public Security (MPS) on 13 March 2025 and came into effect on 1 June 2025.

Highlights of the Measures on Facial Recognition Technology are as follows.

- All data processors should use facial recognition technology only for a specific purpose and of sufficient necessity. If there are recognition methods other than facial recognition to achieve the same purpose or meet the same business requirements, facial recognition technology shall not be provided as the only recognition method.
- Prior to the application of facial recognition technology, data processors shall inform the data subjects of certain information, including the name and the contact information of the data processor, purpose and method of facial information processing and the period for storage of the facial information, etc.
- If the processing of facial information is based on consents of data subjects, the data processors should obtain voluntary, explicit and separate consents from the data subjects.
- Unless otherwise stipulated by laws and administrative regulations or with an individual’s separate consent, data processors should store facial information locally with the facial recognition equipment and should not transmit the facial information through the internet.
- A data processor should make a filing to the authorities about its facial recognition activities if the amount of facial information processed by it reaches 100,000 people.

After release of the Measures on Facial Recognition Technology, on 28 May 2025, the CAC released an Announcement about Filing of the Application of Facial Recognition Technology. Data processors meeting the filing threshold should make their filings on an officially designated website.

In practice, some data processors may use facial recognition technology for HR operation without a necessity check. For example, some companies adopt facial recognition technology for the purpose of checking on

employee attendance without any alternative. Such adoption bears compliance risk under the Measures on Facial Recognition Technology and should be reconsidered. For data processors using applications that store the facial information of more than 100,000 people, it is suggested that their compliance department start preparing for filing materials together with other internal departments such as IT and the relevant business units.

Cross-border data transfers

Certification of cross-border provision of personal information

The Measures on Certification of Cross-Border Provision of Personal Information (the “Measures on the Certification”) was released by the CAC on 14 October 2025 and came into effect on 1 January 2026. It provides rules about certification, the most recently clarified mechanism for cross-border data transfer under Chinese law.

Article 38 of the PIPL designed three mechanisms for cross-border data transfer, including:

- security assessment;
- standard contract filing; and
- certification of cross-border provision of personal information.

The rules on the first two mechanisms were released years ago; the rules on the certification of cross-border provision of personal information have long been absent in practice. It seems that adding this mechanism does not cause any difference in practice.

Highlights of the Measures on the Certification include the following.

- The measures clarify the procedures required to qualify as a professional certification institution. Names of those qualified institutions will be published through official channels.
- Data processors that transfer personal information overseas shall complete the personal information protection impact assessment (PIPIA) covering contents required by the Measures on the Certification.

- The validity period of a certification is three years and can be extended by filing an application six months prior to the expiration of the validity period.

Following the Measures on the Certification, CAC announced only three qualified professional certification institutions as of January 2026.

Official Q&As from CAC on cross-border data transfers

In 2025, CAC released two lists of Q&As to provide explanation about frequently asked questions concerning cross-border data transfers, in April and October, respectively. The practice of cross-border data transfers has stabilised, and compliance burdens regarding cross-border data transfers are reducing.

The April Q&As list offered a broader policy overview and high-level clarification of the Chinese cross-border data transfer mechanism. It explains that China's data export regime is to ensure secure and free flow for business needs, while regulating transfers involving personal information and important data. It also highlights key supporting measures, such as the Free Trade Zone (FTZ) negative list system, which exempts certain data from standard compliance paths and specifies that important data is not prohibited from leaving but requires a security assessment process in accordance with the law. The April Q&As list also shares ways to raise the efficiency for multinational corporations in their cross-border data transfer, such as consolidated group filings and the forthcoming personal information protection certification mechanism.

On the basis of the April Q&As, the October Q&As list further clarifies business scenarios that can be exempted from the cross-border compliance mechanism. For example, cross-border shopping or exams are not limited to the examples listed in the law, but must meet two core conditions: they must be for concluding or performing a contract with an individual being the counterparty; and the transfer must be based on the principles of being minimal and necessary. The October Q&As list explicitly states that domestic hotel bookings for domestic individuals do not qualify for the exemption. The October Q&As list also addresses specific operational questions, con-

firmed that data processing system upgrades alone do not trigger reassessment.

Increased focus on AI governance

In 2025, Chinese authorities continued AI governance, focusing on the labelling of AI-generated content. This was not the first mention of labelling requirements for AI-generated content. In the Administrative Provisions on Deep Synthesis of Internet-based Information Services released in 2022, the legislation already stipulated that, for contents that may cause confusion or misidentification by the public, prominent labels shall be added to demonstrate that the contents are AI generated or edited. However, the standard for such labelling was not specified in the 2022 regulation.

On 7 March 2025, the CAC, together with the Ministry of Industry and Information Technology (MIIT), the MPS and the State Administration of Radio and Television (SART), released the Measures on Labelling AI-Generated or Composed Content (the "Measures on Labelling"), which came into effect on 1 September 2025.

Highlights of the Measures on Labelling include the following.

- The measures divided AI labels into explicit labels and implicit labels, and specified where to add explicit labels for different types of content, including text, voice, picture, video, virtual scene, etc. They also specified contents to be included under the implicit labels.
- Different obligations are set for different parties, including the AI generation service providers that provide online information content dissemination services, the internet application distribution platform and users who upload AI-generated contents.

Apart from the Measures on Labelling above, a compulsory national standard Cybersecurity technology – Labelling method for content generated by artificial intelligence (GB 45438-2025, the "Labelling Method") was also released in 2025, which provided more detailed instructions from a technology perspective and examples for different scenarios. The Labelling Method can be taken as a reference for companies

that need to design the label for AI-generated contents in practice.

Law enforcement and judicial judgments

More frequent inspections on apps, mini programs and software development kits (SDKs)

The governmental authorities continue carrying out compliance inspections on publicly available apps, mini programs and SDKs to enforce personal information protection laws. If the issues raised are not mitigated on time (usually from two weeks to one month), the authorities will take the apps, mini programs and SDKs down from the app stores.

The most common non-compliance issues include the following:

- inadequate privacy policies;
- illegal collection of personal information;
- excessive device permission requests; and
- failure to respond to individuals' requests to uphold their personal information rights.

Judicial cases concerning AI indicate the obligation of service providers

Following the trend in 2024, judicial cases concerning AI are also on the rise in China in 2025, especially involving copyright issues. In 2024, several cases ruled that the AIGC tool provider was found liable for infringing the copyright of certain IP due to not exercising a "reasonable duty of care".

In 2025, a similar case in Shanghai ruled that the AIGC tool provider did not incur liability. In this case, the plaintiff was the IP owner, and a user of the AIGC tool uploaded around 20 pictures of the copyrighted contents to the platform, used the LoRA training function of the tool and generated a LoRA model of the IP, which can produce pictures of the IP contents. Both the user and the AIGC tool provider were sued by the plaintiff for infringement of copyright. The court ruled that the AIGC tool provider incurred no liability because the AIGC tool provider had notified the user about their own obligation, designed a mechanism to receive complaints, and delisted the related LoRA model after receiving infringement notice from the plaintiff. Therefore, the court considered that the AIGC

tool provider had taken necessary measures and was not liable for infringement.

This case demonstrates that the AIGC tool provider may avoid legal liabilities by establishing necessary risk control measures. The practice of the AIGC tool provider in such cases can be taken as a reference for similar service providers.

The first case on MNCs for non-compliant cross-border transfer of personal information

In September 2025, Shanghai authorities issued an administrative punishment against a famous global luxury brand's affiliate in Shanghai, for three illegal activities:

- customer personal information was transferred overseas without completing the cross-border mechanism;
- customers were not fully informed about the cross-border data transfer, and separate consent was not obtained; and
- technical security measures such as encryption and de-identification were not implemented.

The announcement published by the authorities is short and did not disclose much information. According to a piece of public information, in May 2025, the luxury brand was reported to have had a data leak by multiple media and its customers in China also received relevant text alerts. Such a leak may be the reason the authorities started an investigation and discovered the compliance defects regarding cross-border data transfer.

Despite the authorities long reminding businesses about complying with the cross-border mechanism, there were few penalty cases in practice for non-compliance with such a statutory requirement. This case shows that Chinese authorities have started to check and punish multinational businesses for not being compliant with the cross-border mechanism. Those who have not fulfilled their obligations under such a mechanism should rectify the non-compliance as soon as possible.

What to expect in 2026

It is expected that the legal developments on data security and personal information protection in 2026 will continue to be shaped by the need to grow the domestic economy, adaptive to technological innovations and affected by the evolving global politics and interactions. The focus will remain on balancing already robust and aggressive data protection with the pressure to grow the domestic economy and take the lead in international technical innovation.

For multinational companies that are operating businesses in China, it is worthwhile keeping a closer watch on the law enforcement developments and trends than the development of the laws themselves.

EGYPT

Law and Practice

Contributed by:

Ibrahim Shehata, Hesham Kamel, Mohamed Abed and Omar Selim
Shehata & Partners



Contents

1. Legal and Regulatory Framework p.72

- 1.1 Overview of Data and Privacy-Related Laws p.72
- 1.2 Rights and Obligations p.73
- 1.3 Special Categories of Personal Data p.74
- 1.4 Processing of Personal Data for Research and Development Purposes p.75
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.75
- 1.6 Data Breach Requirement p.75
- 1.7 Regulators p.76
- 1.8 Enforcement Proceedings and Fines p.77
- 1.9 Enforcement Trends p.77

2. Privacy Litigation p.77

- 2.1 Privacy Litigation Overview p.77
- 2.2 Recent Case Law p.77
- 2.3 Collective Redress Mechanisms p.78

3. Requirements for the Protection and Processing of Non-Personal Data p.79

- 3.1 Objectives and Scope of Data Regulation p.79
- 3.2 Interaction of Data Regulation and Data Protection p.80
- 3.3 Rights and Obligations Under Applicable Data Regulation p.80
- 3.4 Regulators and Enforcement p.81

4. Sectoral Topics p.81

- 4.1 Use of Cookies p.81
- 4.2 Personalised Advertising and Other Online Marketing Practices p.81
- 4.3 Employment Privacy Law p.82
- 4.4 Data Protection in M&A p.82

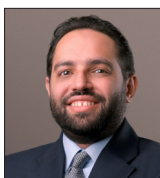
5. International Considerations p.83

- 5.1 Restrictions on International Data Transfers p.83
- 5.2 Government Notifications and Approvals p.83
- 5.3 Data Localisation Requirements p.84
- 5.4 Blocking Statutes p.84
- 5.5 Recent Developments p.85

Shehata & Partners was founded in 1996 and has been driven by a vision of providing unique legal services that cater to the business needs of corporate entities doing business in Egypt. Its core mission is to provide the most trusted and effective legal advice on both dispute resolution and corporate law in

Egypt. The firm is result-driven and delivers exceptional services to clients across various practice areas and multiple industries. It continues to achieve the highest client satisfaction rates in the region due to the meticulous implementation of its client-centric approach.

Authors



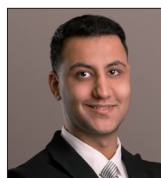
Ibrahim Shehata is a partner at Shehata & Partners, and has accumulated more than a decade of experience within the Egyptian market. He started his career with Ibrachy & Dermarkar and then

Sharkawy & Sarhan law firms before earning his Master of Laws degree in International Arbitration and Venture Capital from New York University. He focuses on corporate law, where he has successfully advised several multinational companies on doing business in Egypt. In the last few years, Ibrahim has been one of the key players in the entrepreneurial ecosystem, helping both start-ups and venture capital firms navigate legal issues and become more investment-ready.



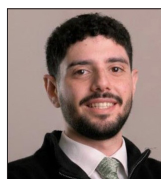
Hesham Kamel is a partner at Shehata & Partners, based in Paris, France, and has more than seven years' experience in corporate governance, projects, manufacturing, privacy, personal data and

cybersecurity. He has significant academic leverage, as he holds two master's degrees from the Sorbonne Law School, both specialising in the international rules governing business and trade. Hesham started his career at Sharkawy & Sarhan before joining Shehata & Partners. He has closed several investment rounds with multiple start-ups, and has also been an integral part of multimillion-dollar investment projects.



Mohamed Abed is an associate at Shehata & Partners. He graduated with honours from Tanta University's Faculty of Law (English Department), ranking fourth in his class. He also holds a Master's degree in Public

Law. Prior to joining S&P, Mohamed gained valuable experience through internships at prestigious law firms and in-house legal departments, exposing him to various legal areas such as corporate law, contract negotiation, labour law and regulatory compliance. He now specialises in corporate law, labour law and contract drafting, assisting clients with legal documentation, regulatory compliance and employment matters.



Omar Selim is an associate at Shehata and Partners, focusing on data protection, corporate and labour law matters, with strong experience in drafting and negotiating commercial agreements, including shareholders'

agreements, ESOP plans and software-related contracts. He is experienced in corporate structuring, transactional work and the execution and termination of commercial arrangements, adopting a practical, business-oriented approach. He has worked on major projects within private and public free zones, advising multinational companies on regulatory compliance, project implementation and cross-border corporate matters.

Shehata & Partners

Cairo Business Plaza
North Tower
2nd Floor, Unit 204
New Cairo
Cairo
Egypt

Tel: +2 28 135 692
Email: info@shehatalaw.com
Web: shehatalaw.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Data Protection and Privacy Law Sources in Egypt

The Personal Data Protection Law issued under Law No 151 of 2020 (PDPL), together with its executive regulations issued by the Minister of Telecommunication and Information Technology Decree No 816 of 2025 (“Regulations”), constitute the primary legal source governing data protection and privacy in Egypt. The PDPL is further supported by constitutional provisions and other complementary legislation.

Constitutional foundation

The Constitutional foundation of the PDPL is based on three provisions:

- Article 28, stipulating that information-based activities are key components of the national economy, and that the State commits to protecting them and increasing their competitiveness;
- Article 31, stipulating that the security of information space is an integral part of the system of national economy and security; and
- Article 57, stipulating that private life is inviolable, which extends to electronic correspondence, the confidentiality of which is guaranteed. Furthermore, the State shall protect the rights of citizens to use all forms of public means of communication.

The Telecommunications Law

The Telecommunications Regulation Law No 10 of 2003 recognises the right to privacy within the telecommunications sector by reinforcing the confidentiality of communications, notably through Article 73, which criminalises the unlawful disclosure of the content of communications or information relating to users of telecommunications networks.

The Cybercrimes Law

The Cybercrimes Law No 175 of 2018 constitutes a complementary legislative source of the PDPL, as it establishes direct criminal protection for personal data and the right to privacy. In particular, Article 25 criminalises the unlawful disclosure or use of personal data and any conduct that violates individuals’ privacy without their consent, while Article 26 imposes enhanced penalties for the misuse of information technology in processing personal data in a manner that harms a person’s reputation or dignity.

Interaction Between Data and Privacy Laws Across Different Levels of the Legal System

Sector-specific laws, including the Telecommunications Law and the Cybercrimes Law, may intersect with the PDPL where personal data is processed, secured, retained or disclosed within regulated sectors. This intersection commonly arises in matters relating to confidentiality of communications, data security measures, data retention obligations and unlawful access or disclosure. In such cases, the PDPL establishes the general data protection principles, while sector-specific laws impose complementa-

ry or more detailed obligations, provided they remain consistent with the PDPL and the constitutional right to privacy.

Moreover, the PDPL excludes from its scope of application personal data retained by the Central Bank of Egypt and the entities falling under its jurisdiction (except for money transfer and currency exchange companies), as well as data retained or claimed by the Egyptian Presidency, Ministry of Interior, Ministry of Defence, General Intelligence Service and Administrative Control Authority. The PDPL also excludes personal data related to judicial seizure reports, investigations and lawsuits.

Extraterritorial Reach of the PDPL

The PDPL's extraterritorial scope is based on nationality, residence and effects-based criteria, as set out in its second article of issuance.

Under this framework, the PDPL applies to Egyptian nationals who commit any of the offences stipulated therein, regardless of whether such offences are committed in Egypt or abroad. It also applies to non-Egyptian nationals residing in Egypt, irrespective of whether the offence occurs inside or outside Egypt.

Furthermore, it extends its arm to non-Egyptian nationals residing abroad, provided that the following conditions are met:

- one of the offences stipulated under the PDPL has been committed;
- the same act is punishable under the law of the country where it was committed, irrespective of its legal characterisation; or
- the personal data concerned relates to Egyptian nationals or to foreign nationals residing in Egypt.

1.2 Rights and Obligations

General Principles and Requirements for Processing Personal Data

Licensing and approval requirements

The collection and processing of personal data is subject to the requirement that the entity carrying out such activities be duly licensed as a data controller and/or processor. Approval must also be obtained from the Personal Data Protection Center for the mechanisms

used to collect personal data, and for the method of obtaining the consent of the data subject.

General requirements

Personal data must be:

- collected for lawful, specific and declared purposes;
- accurate, valid and adequately secured;
- processed in a lawful and appropriate manner consistent with the purposes for which it was collected; and
- not retained for a period longer than necessary to achieve the specified purpose.

Furthermore, the processing of personal data must be made on one of the legal bases permitted by the law, which include obtaining the data subject's consent, executing a contractual or legal obligation, pursuing a legal action, abiding by an order of a court of an investigation authority, or legitimate interest.

Data Subject's Rights

Under Article 2 of the PDPL, personal data may not be collected, processed, disclosed or made available by any means except with the explicit consent of the data subject or in cases expressly permitted by law. In this context, the data subject is granted the following rights:

- the right to be informed of, access, review and obtain personal data held by any data holder, controller or processor;
- the right to withdraw consent previously given for the retention or processing of personal data;
- the right to request the correction, amendment, updating, addition or deletion of personal data;
- the right to limit the processing of personal data to a specific scope;
- the right to be informed of any breach or violation affecting personal data; and
- the right to object to the processing of personal data or its outcomes where such processing conflicts with the data subject's fundamental rights and freedoms.

Except for the right to be informed of data breaches, the exercise of these rights may be subject to a ser-

vice fee payable by the data subject to the controller or processor, as determined by the Center and within the legally prescribed limit.

The practice of the Center in the future might lead to the generation of more specific rights for data subjects, based on its interpretation and the implementation method of the law.

Main Compliance “To-Dos” for Organisations

While it is difficult at this early stage of the PDPL's implementation to make an exhaustive to-do list for organisations, the following actions require attention.

- Updating the existing privacy policies to meet the requirements of the Regulations – eg, specifying the scope of collecting and processing the data and the nature of collected data, implemented procedures in case of data breaches, and cross-border transfer of data.
- Collecting and recording the written and explicit consent of data subjects in readily accessible records that comply with the standards set out in the Regulations.
- Conducting a comprehensive assessment of the data held, in terms of relevance, accuracy and recency, deleting or anonymising unnecessary data to reduce regulatory risk, and documenting such actions. In case of deletion, there is a requirement to notify the data subject of such.
- Appointing a data protection officer (DPO) and providing appropriate legal and technical training, with a view to ensuring successful registration with the Personal Data Protection Center. The appointment should be made in writing and grant the DPO sufficient independence to effectively perform their duties.
- Appointing a local representative where operations are conducted in Egypt without an established corporate presence in Egypt.
- Reviewing and reorganising internal access controls, including defining data access rights, hierarchies and systems, to ensure that personal data is accessible only to authorised personnel.
- Developing and implementing a comprehensive data security policy, including technical and organisational measures, incident response procedures,

access controls and periodic reviews, in line with the standards issued by the Center.

- Determining in advance the permits and licences required, and allocating the necessary resources while preparing the relevant documentation and supporting information.
- Designing a notification procedure to ensure compliance with the Regulations timelines for data breach notifications, whether within 72 hours or without delay, as applicable.
- Assessing how personal data is transferred, accessed, shared, circulated or stored outside Egypt, identifying local alternatives where feasible and, where not, ensuring that the hosting country has an adequate data protection framework and that the existing arrangements meet appropriate business, security and compliance standards.
- Introducing data consent and data protection compliance provisions into service agreements, employment contracts and any other agreements involving the sharing of personal data.
- Where applicable, concluding data processing agreements that clearly allocate responsibilities and liabilities between the parties.

1.3 Special Categories of Personal Data

The PDPL identifies certain categories of personal data as sensitive personal data, the processing of which is subject to additional obligations.

Sensitive personal data includes data revealing a person's mental, psychological, physical or genetic health, biometric data, financial data, religious beliefs, political opinions or security status. Children's data is also classified as sensitive.

General Requirements

All activities related to sensitive personal data must meet the following requirements:

- obtaining a permit or a licence from the Center;
- obtaining the explicit written consent of the data subject;
- collected data needs to be essential and necessary for the ultimate purpose of processing (ie, data minimisation), without causing any harm to the data subject;

- abiding by all the requirements and standards issued by the Center; and
- maintaining electronic and secure records of processing activities.

Special Requirements for Children's Data

The PDPL imposes additional requirements for the processing of children's data, as follows.

- If the child is under 15 years old, valid consent must be obtained from the child's guardian in writing and in an explicit manner. Such consent must be limited in time, and may be revoked later on.
- If the child is at least 15 years old, the child, or their guardian, must give their written consent.
- If the child is to participate in a game or a competition, the requested data must be limited to what is strictly necessary. Moreover, such data may not later be used in any operations involving profiling, tracking or behavioural monitoring of children.

Processing of Data Relating to Criminal Convictions and Offences

The PDPL does not apply to criminal convictions and offences, as it expressly excludes personal data relating to judicial seizure records, investigations and judicial proceedings from its scope. Consequently, such data falls outside the regulatory framework of the PDPL.

Under the rules of criminal procedure, investigations conducted by the Public Prosecution are confidential by operation of law. Pursuant to Criminal Procedures Law No 174 of 2025, access to investigation materials and case files is restricted to legally authorised persons whose involvement is required for the conduct of the proceedings, and only to the extent permitted by law.

1.4 Processing of Personal Data for Research and Development Purposes

The anonymisation process is currently not regulated under the PDPL, but may be organised by the Center at a later date. However, data related to persons only constitutes “personal data” – and therefore becomes subject to the PDPL – where it relates to an identified or identifiable individual, including health data. Once such data no longer pertains to an identified or

identifiable individual, it automatically falls outside the scope of the PDPL.

Egyptian law does not provide for a unified or sector-specific regime governing the secondary use, sharing or reuse of health data comparable to the European Health Data Space Regulation. Instead, the applicable legal framework is limited to the general rules set out under the PDPL. As a result, the regulation of secondary uses of health data in Egypt, including the anonymisation of patient data for product development or scientific research, remains contingent on any future decisions, guidelines or regulatory frameworks to be issued by the Center.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Egypt does not currently have a standalone law regulating AI. Accordingly, the use of personal data in the training, development or operation of AI systems or models is governed by the PDPL and its Regulations.

Any processing of personal data in this context must comply with the general data protection principles set out under the PDPL, including lawfulness, purpose limitation, data minimisation, data accuracy, storage limitation, integrity and confidentiality, and accountability.

Specific AI-Related Requirements and Guidance

Under the Regulations, where personal data is used to train or operate AI models, the legal obligation imposed on data processors is limited to compliance with “locally, regionally, and internationally recognised standards”. This includes the Egyptian Charter for Artificial Intelligence, a soft law document issued by the National Council for Artificial Intelligence. This Charter includes the common international standards, such as human-centredness, transparency and explainability, fairness, security and safety, and accountability, and covers the use of AI in both the public and private sectors.

1.6 Data Breach Requirement

A personal data breach includes any unauthorised access, disclosure, copying, transfer, alteration or destruction of personal data during storage, transmission or processing. Once aware of a breach, both

the controller and the processor must take immediate action.

Mandatory Notification

The Center must be notified within 72 hours of becoming aware of the breach. Where the breach relates to national security considerations, notification must be made without delay. Notification must be submitted through the designated channels and recorded in a secure breach register, and must include details of the breach, affected data, potential impact, mitigation measures and the DPO's details.

Affected data subjects must be notified within three working days of notifying the Center, with information on the breach and the measures taken.

Required Actions

Organisations must:

- assess and contain the breach;
- notify the Center within the statutory timeframe;
- notify affected data subjects;
- document the breach and corrective actions;
- implement technical and organisational measures to prevent recurrence; and
- ensure oversight by the DPO.

Investigations and Liability

The Center may investigate breaches, request information and co-ordinate with national security authorities where applicable. Non-compliance may result in regulatory, administrative or criminal sanctions.

1.7 Regulators

Personal Data Protection Center

The Personal Data Protection Center is the primary authority responsible for enforcing the PDPL and its Regulations. It regulates activities related to personal data processing, issues the required permits and licences, makes national policies and guidelines, and investigates violations.

However, as it was only established recently, and there is currently a grace period extending until 31 October 2026, the Center is not yet fully utilising its regulatory powers.

In all cases, the Center has the power to make investigations based on complaints it receives or at its own discretion. Moreover, the Center is duly authorised to effect settlements of claims and to enter into reconciliation agreements in respect of criminal proceedings with the parties concerned.

The Center co-ordinates domestically with sectoral regulators and national security authorities. It may also co-operate with foreign data protection authorities pursuant to international, regional or bilateral agreements or based on reciprocity, for the purposes of protecting personal data, verifying compliance by controllers and processors outside Egypt, exchanging information and assisting in the investigation of data breaches and related offences.

National Telecommunications Regulatory Authority (NTRA)

The NTRA is responsible for overseeing privacy and confidentiality obligations within the telecommunications sector in accordance with the Telecommunications Law. Its mandate includes ensuring that telecom operators comply with legal requirements relating to the protection of users' communications and personal data.

Regulatory action by the NTRA may be triggered either by complaints submitted by users or through the NTRA's own monitoring and supervisory activities. In this context, the NTRA is empowered to conduct audits and inspections of telecommunications operators and to impose regulatory or administrative sanctions where breaches are identified.

Authorities Responsible for the Enforcement of the Cybercrimes Law

As described in **1.1 Overview of Data and Privacy-Related Laws**, the Cybercrimes Law contains some provisions that are related to data privacy, especially when concerned with an individual's reputation and private life. In this regard, the authorities responsible for enforcing the Cybercrimes Law include the Public Prosecution, the economic courts and the NTRA.

1.8 Enforcement Proceedings and Fines

As indicated in 1.7 **Regulators**, the Center is not currently utilising its full powers, due to the grace period extending until 31 October 2026.

The PDPL allows the Center to initiate investigations and enforcement actions under the PDPL. Proceedings may also be triggered by complaints submitted by data subjects, or data breach notifications filed by controllers or processors.

The Center may refer the cases it handles to the economic courts, which are the competent courts with respect to applying the criminal sanctions contained in the PDPL. This is without prejudice to the claimant's right to request civil compensation.

The Center may also apply administrative sanctions. This starts by delivering a warning to the person found to be in violation of the PDPL, requiring them to comply with its provisions within a specified duration. If this duration lapses without such person having complied with the PDPL, the Center may deliver another warning, suspend or revoke the licence/permit, and subject the person concerned to its scrutiny.

1.9 Enforcement Trends

Effective Enforcement of the PDPL

The most significant development has been the issuance and entry into force of the Regulations in November 2025, which triggered the grace period extending until 31 October 2025, while starting to implement the PDPL.

Launch of the Center's Online Platform

The launch of the Center's official online platform (pdpc.gov.eg) represents an important step in operationalising the data protection framework. The platform shall function as a central point for regulatory information, guidance, licensing-related updates, and communication with regulated entities, enhancing transparency and accessibility.

Issuance of Guidelines by the Center

The Center has published new guidelines and model forms, with the purpose of spreading awareness of the implementation of the PDPL. By way of illustration, the guidelines include an explanation of core concepts

such as the data subject's consent, the legal foundations for processing data, the role of a DPO, privacy policies, and permits and licences.

While these guidelines are not legally binding, they reflect the orientations of the Center in the implementation of the PDPL.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Privacy and data protection litigation in Egypt remains at an early stage. To date, judicial practices are limited. There has been a recent case before the Economic Court of Alexandria (see 2.2 **Recent Case Law**), but this still does not yet amount to a settled or consistent line of case law. However, it reflects an emerging judicial willingness to engage with privacy and data protection arguments, especially in regulated sectors that process large volumes of personal data.

Compensation for Non-Material Damage

Egyptian law expressly recognises compensation for non-material damage, including psychological, reputational and emotional harm arising from privacy violations. Such damage is considered compensable in privacy-related claims.

Non-material damage is assessed at the discretion of the court, taking into account the seriousness of the violation, the nature and sensitivity of the data involved, and the impact of the infringement on the claimant's dignity, privacy and mental well-being.

Possibility of Privacy Claims

Affected individuals may file a complaint with the Center, and can also bring a civil claim directly before the competent courts seeking compensation, without prejudice to their right to pursue judicial remedies.

2.2 Recent Case Law

In September 2025, prior to the issuance of the Regulation, the Economic Court of Alexandria issued a landmark judgment ordering the defendant to pay EGP10 million in compensation for the unlawful compromise of a customer's personal data. Although the case was

brought against a telecommunications operator, it has significant implications in terms of data privacy laws.

The Court held that a company may incur civil liability for data protection violations, even during the previous absence of the Regulations. Liability was established by the Court under general tort law, and compensation was awarded without any statutory cap, as civil indemnification is not subject to the limits applicable to criminal fines.

Enforcement Through Custodian's Liability

The Court characterised the defendant as the custodian (controller) of the claimant's personal data and applied the doctrine of the custodian's liability, which does not require proof of fault. Liability may only be avoided by proving an external cause beyond the custodian's control. Allegations of fraud, employee error or technical failures were held insufficient to exempt the company from liability.

As a result, the company was deemed responsible for failing to prevent unauthorised access, misuse and manipulation of the claimant's personal data, and was required to exercise a heightened duty of care reflecting its professional position.

Implications for Data Privacy

The judgment signals a shift in the judicial approach to the enforcement of the PDPL, with the following key implications:

- liability without fault may be imposed for personal data breaches on the basis of the custodian's liability;
- defences are narrowly construed, and internal failures or third-party fraud may not absolve liability; and
- financial exposure is significant, with compensation awards potentially reaching millions of Egyptian pounds.

2.3 Collective Redress Mechanisms

There is no general legislative framework allowing a claim to be brought on behalf of an undefined group of affected persons, including in privacy or data protection matters.

Procedural Alternatives to Collective Redress

Multiple claimants in a single action

Under the Civil and Commercial Procedures Law, multiple claimants may bring a single action where the subject matter or legal cause is common or closely connected. Each claimant must individually establish standing, damage and causation. This mechanism does not constitute collective redress in the technical sense.

Regulatory complaints

In data protection matters, data subjects may file complaints with the Center. The Center's decisions are administrative in nature and do not amount to judicial collective redress or collective compensation.

Admissibility Criteria

All claims must satisfy the general requirements of standing and direct personal interest. Egyptian law does not provide a mechanism for certifying a representative claimant or aggregating claims of persons who are not formally parties to the proceedings.

Indicative Timelines

Actions involving multiple claimants follow the ordinary timelines of civil litigation. There are no expedited or special procedural rules for claims with a collective dimension, and proceedings may be lengthy, particularly where technical expertise is required.

Typical Relief

Available remedies include:

- monetary compensation, assessed individually for each claimant based on the damage suffered;
- injunctive or corrective orders to cease unlawful conduct; and
- regulatory or administrative measures imposed by competent authorities.

Egyptian law does not provide for collective or aggregate damages awarded to an undefined group.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

There is no general legal framework governing the protection or processing of non-personal data, similar to the EU Data Act. The PDPL, its Regulations and the mandate of the Center are limited to personal data and do not extend to non-personal data.

Adoption and Scope of the Open Data Policy

Against this backdrop, Egypt has adopted an Open Data Policy (the “Policy”), issued by the National Council for Artificial Intelligence in 2025. The Policy defines open data as non-sensitive and non-personal data held by the governmental authorities and made available in an electronic-readable format, subject to minimal restrictions on its use or reuse. However, the Policy serves as a transitional regulatory instrument, pending the issuance of a comprehensive data governance law, its executive regulations, and the accompanying data classification framework; the Policy is expected to be superseded and replaced by such law, once enacted.

In this context, the Policy aims to support and promote the development of innovative digital services. It specifically regulates the availability of data not falling within the categories of personal data, data related to national security, and trade secrets. Once enacted, the anticipated data governance law and its executive regulations are expected to designate the Egyptian Data Governance Authority (which is not yet established) as the central co-ordinating authority, responsible for setting priorities, monitoring compliance, overseeing the availability of public data sets, and approving relevant strategic initiatives.

Overall, the Policy primarily addresses data access, use and reuse, rather than establishing rules governing the processing of non-personal data.

Internet of Things Regulatory Framework

The NTRA issued a dedicated internet of things (IoT) regulatory framework in Egypt in January 2022, setting out the key rules and procedures governing the provision and use of IoT services and expressly providing that the regulatory framework shall be imple-

mented in accordance with, and abide by the terms of, the PDPL, its Regulations, the Cybercrimes Law and the Telecommunications Law. In addition, the framework expressly prohibits any user of IoT services from transferring IoT-related data outside Egypt.

In practice, IoT services may involve the access and sharing of data with the governmental authorities. Where such IoT-generated data does not relate to identified or identifiable individuals and does not qualify as sensitive data, it may be classified as non-personal, non-sensitive data. In such cases, access to and reuse of this data would be expected to fall within the scope of the Policy.

By way of example, data generated by the IoT sensors installed by a government authority to monitor traffic flow, air quality or energy consumption levels, where the data is aggregated and does not allow for identifying individuals, would generally be considered non-personal and non-sensitive, and may therefore be made available in accordance with the Policy.

Regulatory Framework for Cloud Services and Data Centres

With respect to cloud computing, Egypt has a multi-layered regulatory and policy approach. The NTRA has established a regulatory framework governing the establishment and operation of data centres and the provision of cloud computing services in Egypt. This framework aims to attract large-scale data centres and cloud service providers, and to support Egypt’s broader digital transformation objectives.

Cloud First Policy

In parallel, the Supreme Council of Digital Society (SCDS), formed under President Decree No 501 of 2017, adopted the Cloud First Policy in 2024. This guiding non-binding policy was developed and implemented in alignment with international standards and best practices.

The Cloud Policy is aligned with Egypt’s Vision 2030 and the Digital Egypt Strategy, and aims to highlight the pivotal role of cloud computing in building a secure and sustainable digital society. The Cloud Policy also contributes to promoting the adoption of cloud computing services across both the public and

private sectors, leveraging their advantages in developing software, enhancing workforce capabilities and improving service efficiency. It also accelerates the pace of secure data migration and the use of data through public cloud computing systems.

Data Classification and Future Legislative Developments

Through its executive office and specialised committees, the SCDS continues to undertake efforts to prepare a draft law establishing binding rules and standards for the classification, availability and exchange of official data and information. In addition, the Cloud Policy emphasises that proper data classification is a core pillar of effective cloud computing governance. Given the significance of data classification, work is currently underway to prepare the draft law mentioned above. Pending the issuance of this legislation, the Cloud Policy adopts an interim data classification approach aligned with international standards, and classifies data into four levels: public, confidential, secret and top secret.

For the purposes of the Cloud Policy, public data refers to public data that held by the governmental authorities and available for general access. Accordingly, such data would fall within the scope of the Open Data Policy and be subject to its rules on access, use and reuse.

3.2 Interaction of Data Regulation and Data Protection

With respect to the legal basis and confidentiality of personal data, Egyptian law adopts a clear hierarchy. Where data processed under IoT or cloud computing frameworks qualifies as personal data, the legal basis for processing and the confidentiality obligations are governed solely by the PDPL and its Regulations. However, sector-specific frameworks (ie, IoT or cloud computing) do not create independent legal bases for processing personal data and instead defer to the PDPL.

Moreover, in the absence of a dedicated non-personal data protection regime in Egypt, non-personal data must meet specific requirements in order to be treated as a trade secret under the Intellectual Property Law No 82 of 2002. In particular, the data must:

- have commercial value as a result of not being publicly available;
- be known only to a limited group of persons; and
- be subject to reasonable measures taken by its holder to preserve its confidentiality, including the use of confidentiality agreements with employees and business partners.

Alternatively, such data may be registered as a copyright, provided that it fulfils the legal and regulatory conditions.

3.3 Rights and Obligations Under Applicable Data Regulation

In the absence of a clear legislative framework in Egypt governing the rights and obligations relating to the use of non-personal data, other than the Open Data Policy discussed in **3.1 Objectives and Scope of Data Regulation**, and pending the issuance of the anticipated data governance law, the existing regulatory frameworks applicable to IoT and cloud computing primarily operate by reference to the rules governing personal data, to the extent that any personal data is involved.

Accordingly, the current rights and obligations under these frameworks largely relate to the use of personal data, as regulated by the PDPL, its Regulations and the guidelines issued by the Center. In this context, Article 2 of the PDPL establishes a set of fundamental rights granted to data subjects (see **1.2 Rights and Obligations** for more detail). At present, the PDPL expressly provides for the right of access, while the remaining rights are not explicitly detailed. However, the Center is expected to further clarify and address such rights through the issuance of additional specific guidance.

Articles 4 and 5 of the PDPL and Articles 3 and 4 of its Regulations set out the core obligations applicable to personal data users, whether acting as controllers or processors. These provisions establish the main responsibilities governing the lawful use of personal data, including, in particular:

- obtaining the relevant licences or permits;
- the obligation not to unlawfully disclose personal data;

- the appointment of a DPO, where required;
- notifying data subjects of personal data breaches;
- compliance with enhanced obligations relating to sensitive personal data;
- specific protections for children's personal data;
- restrictions and conditions on cross-border data transfers;
- obligations applicable to direct marketing activities;
- requirements governing the use of visual surveillance methods in public spaces; and
- the obligation to appoint a representative in Egypt, where applicable.

3.4 Regulators and Enforcement

In Egypt, the competent authority responsible for enforcing the regulatory frameworks applicable to IoT and cloud computing services is the NTRA. In exercising its mandate, the NTRA co-ordinates with privacy and competition authorities by requiring compliance with the PDPL, its Regulations and, recently, the guidelines issued by the Center, as well as with the rules governing competition law in Egypt.

In addition, the NTRA and the Egyptian Competition Authority signed a memorandum of understanding to enhance co-ordination and strengthen the protection of free competition in Egypt's telecom market through a joint executive committee. The co-operation aims to prevent anti-competitive and monopolistic practices, ensure fair regulation of the ICT sector, and maintain high-quality telecom services at fair prices for users. It also seeks to support digital transformation while attracting new investments and safeguarding existing ones.

From a competition perspective, Articles 2, 24 and 30 of the Telecommunications Law establish core principles for the protection of free competition in the telecommunications sector, including:

- the obligation for licensed operators to provide services under conditions of free and fair competition;
- the prohibition of cross-subsidisation of one service at the expense of another; and
- the requirement to provide services to users without discrimination.

The Telecommunications Law further entrusts the NTRA with determining the thresholds beyond which anti-competitive or monopolistic practices may arise within the sectors it regulates.

Recent regulatory trends in Egypt include the issuance of the Regulations of the PDPL and the launch of the official website of the Center, which provides practical guidance to stakeholders. These guidelines address key compliance areas, including but not limited to data subject consent, obligations of data users (controllers and processors), data protection principles, and the lawful bases for processing personal data. Collectively, these developments reflect a shift toward greater regulatory clarity, operational guidance and enforcement readiness in the data protection landscape.

4. Sectoral Topics

4.1 Use of Cookies

Under the general principles of the PDPL, the use of online tracking technologies – including cookies, SDKs and other device identifiers – requires obtaining the prior, explicit and valid consent of the data subject. Where such technologies are used for marketing purposes, they are also subject to the rules on electronic direct marketing.

Consent must be obtained through fair and transparent means. Misleading consent practices, including dark patterns or interfaces designed to influence user choices, invalidate consent, as it cannot be considered freely given, explicit or informed.

Each electronic marketing communication must include a clear and effective “unsubscribe” mechanism. Where such a mechanism exists in form but is ineffective in practice, or where marketing communications are disguised as personal messages, the processing is unlawful.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised or targeted advertising in Egypt is regulated under the PDPL as a form of direct electronic marketing whenever it is based on an individual's data, behaviour or profiling.

Personalised or profiling-based advertising is prohibited without the data subject's prior explicit consent. Marketing communications must:

- clearly identify the sender;
- state that they are sent for direct marketing purposes;
- include a valid contact address; and
- provide clear and easy mechanisms that allow the individual to refuse the communication or withdraw consent at any time.

The PDPL also:

- requires marketers to limit the use of data to the specific marketing purpose for which consent was given;
- prohibits the disclosure of the data subject's contact details; and
- obliges marketers to retain electronic records evidencing consent, its amendments or withdrawal for three years from the date of the last marketing communication.

Any use of profiling for marketing purposes falls within this regime and requires compliant prior consent. The use of sensitive personal data or children's data for personalised or targeted advertising is subject to stricter legal restrictions and enhanced safeguards, and is generally high-risk and highly limited under Egyptian law.

4.3 Employment Privacy Law

There is no specific or settled guidance directly addressing the protection of employee and applicant data. However, based on the current legal framework and prevailing practice, the following principles apply.

Personal data collected during recruitment and job applications is protected under the PDPL even before an employment relationship is formed. Employers must:

- limit processing to recruitment purposes;
- define appropriate retention periods; and
- not reuse or share applicants' personal data without a valid legal basis, in accordance with the PDPL and constitutional protections of privacy.

The existence of an employer–employee relationship does not remove the employee's right to privacy. Employers act as data controllers and may process employee personal data only for lawful, specific and legitimate purposes, and only to the extent necessary and proportionate, in accordance with the PDPL.

Employee monitoring, including time tracking and attendance systems, is permitted where it is necessary for work organisation, wage calculation or legal compliance, provided employees are informed in advance. Hidden, excessive or continuous monitoring may be prohibited, as it could violate the principle of necessity under the PDPL.

Remote work does not expand the employer's monitoring powers. Employers may monitor working hours or performance only to the extent required to perform the employment contract. Intrusive monitoring, constant surveillance or the use of cameras in the employee's home is not permitted, as it interferes with the employee's constitutionally protected private life and exceeds what is necessary under the PDPL.

Personal data processed through workplace IT systems, such as corporate email, HR platforms and task management tools, falls within the scope of the PDPL. Such data may be used only for the employment-related purposes for which it was collected, and may not be repurposed for broader surveillance or disciplinary objectives without a lawful basis and prior transparency.

Background checks are lawful only where they are directly relevant and necessary for the specific role. Collecting criminal, financial or other sensitive personal data without a clear job-related justification violates the PDPL's restrictions on sensitive data processing and the non-discrimination principles under the Labour Law.

4.4 Data Protection in M&A

While the PDPL does not explicitly mention M&A transactions and asset deals, it is still applicable to such matters. The processing and transfer of personal data in this context may be based primarily on the legitimate interest legal basis, provided that the

processing is necessary, proportionate and balanced against the rights of the data subjects.

During the due diligence phase, personal data may be disclosed only to the extent strictly necessary to assess the transaction, in accordance with the data minimisation principle. Access should be limited, and appropriate confidentiality and security measures must be implemented. Where the data involved qualifies as sensitive personal data, it may not be processed or shared unless the explicit and written consent of the data subject has been obtained, in addition to implementing appropriate confidentiality and security measures.

At the stage of change of control or asset transfer, the transfer of personal data constitutes a new processing activity and must be based on a lawful ground, and personal data may not be used for purposes exceeding those for which it was originally collected without a valid legal basis.

A change in the data controller triggers transparency and notification obligations, including informing data subjects of the change in control or processing purposes and complying with any mandatory notifications to the Center where required by the PDPL.

Following the closing and post-merger integration, the acquiring entity must review and align data processing activities, update privacy notices and policies, and ensure that databases are not merged or reused for new purposes without a lawful basis.

5. International Considerations

5.1 Restrictions on International Data Transfers

Cross-border transfers of personal data in Egypt are regulated under the PDPL and its Regulations. However, the PDPL and its Regulations adopt a broad concept of transfer, which covers any transfer, storage, sharing, disclosure, or making available of personal data, whether for processing, storage or any other purpose.

With respect to the mechanisms and assessments required for cross-border lawful transfers, the PDPL and its Regulations set out the key requirements applicable to any data controller or processor, as follows.

- As a general rule, the PDPL and its Regulations prohibit the transfer, storage or sharing of personal data outside Egypt unless the destination country ensures a level of data protection not less than the level prescribed under the PDPL and its Regulations.
- Notwithstanding the adequacy of the level of protection requirement, cross-border transfers to countries that do not provide an equivalent level of protection may be permitted subject to the explicit consent of the data subject (or their representative), and only in limited cases, specified under Article 15 of the PDPL.
- The controller or processor must obtain a licence or permit from the Center, based on its assessment of the adequacy of the level of protection in the destination country.
- The controller or processor must obtain the consent of the data subject for the cross-border transfer.
- Appropriate technical and organisational measures must be implemented to ensure an adequate level of protection for personal data during transfer, storage or sharing, in line with the scope and nature of the data and the terms of the licence or permit.
- Personal data may only be transferred to the country or countries specified in the licence or permit, and any addition of new countries requires an update of such licence/permit.

Moreover, onward transfers are permitted only where the activities of the relevant controllers or processors are compatible or integrated, or serve a legitimate interest of the parties or the data subject, and provided that the level of legal and technical protection applied by the controller or processor located abroad is not less than the level applicable in Egypt.

5.2 Government Notifications and Approvals

The PDPL and the Regulations set out the conditions, procedures and applicable fees for obtaining a licence or permit from the Center to transfer personal data across borders. However, as a general rule, a licence/

permit authorises the data controller or processor to transfer personal data that has been collected or prepared for processing from within the geographic territory of Egypt to outside its borders.

In addition, the Regulations set out the conditions for the cross-border transfer of personal data for both legal persons and natural persons. With respect to legal persons, obtaining a licence/permit for the cross-border transfer of personal data is subject to specific requirements, including, in particular:

- identification of the destination country;
- information on the nature of the activities of the foreign controller or processor;
- a description of the categories and nature of the personal data involved;
- details of the applicable security measures, storage locations (temporary and final) and data protection safeguards during transfer;
- confirmation of compliance with the applicable cross-border transfer standards and requirements;
- specification of the purpose of the transfer; and
- sufficient information regarding data volumes, retention periods, and storage arrangements, in accordance with the templates issued by the Center.

With respect to natural persons, obtaining a permit for the cross-border transfer of personal data requires the following:

- providing information on the nature and description of the personal data to be transferred, its volume, and the purpose of the transfer;
- identifying the destination country and the applicable retention period;
- setting out the security measures, temporary and final storage locations, and safeguards adopted to protect the data during transfer; and
- demonstrating compliance with the applicable standards, rules and requirements for cross-border data transfers, and providing sufficient details regarding storage arrangements in accordance with the templates issued by the Center.

As part of the licensing process, the procedure for obtaining a licence/permit for the cross-border trans-

fer of personal data, whether for legal persons or natural persons, requires the submission of an application to the Center through the designated electronic portal. The application must include all required information and supporting documents. The Center examines the application and notifies the applicant of its decision, whether approval or rejection, within 90 working days from the date on which all required information and documents are duly submitted.

5.3 Data Localisation Requirements

Any cross-border transfer of personal data is prohibited unless it is carried out in accordance with the conditions expressly set out in the PDPL and its Regulations, and subject to obtaining the required licence or permit from the Center.

In addition, the SCDS's Cloud Policy, including data localisation requirements, has entered into force and recommends that data classified as "top secret" or "secret" be hosted exclusively within Egypt. This applies to data related to national security or sensitive operations, and aims to ensure maximum protection against unauthorised access, breaches or manipulation.

5.4 Blocking Statutes

Blocking statutes and foreign judgment control rules are not commonly recognised under Egyptian law in the same manner as in some other jurisdictions. Egypt is not a party to the Hague Evidence Convention, which governs how courts in one state request evidence located in another. In this regard, the analysis below refers to the closest existing legal concepts under Egyptian law that address similar issues.

Judicial Co-Operation and Mutual Legal Assistance

Under the Criminal Procedural Law, judicial authorities may co-operate with their foreign counterparts in the investigation and prosecution of crimes through mutual legal assistance requests. In this regard, the Criminal Procedural Law provides that a request for judicial assistance submitted by a foreign authority may be granted only where it relates to an offence punishable under the law of the requesting state, and where the execution of such a request does not preju-

dice Egypt's security, sovereignty, public order, public morals or national security interests.

Foreign Discovery and Cross-Border Disclosures

In relation to foreign discovery, for example, Egypt and the United States are parties to a mutual legal assistance agreement in criminal matters, which provides that where one of the two States requests data relating to the identity or location of individuals, the requested State is obliged to provide such information in accordance with the terms of the agreement.

Sanctions Compliance

From a sanctions compliance perspective, the Criminal Procedural Law allows Egyptian authorities to refuse a request for judicial assistance where the offence forming the subject of the request is not punishable under Egyptian law.

Interaction With the PDPL and Judicial Co-Operation Exceptions

The PDPL expressly provides that its provisions do not apply to personal data relating to judicial records, investigations or judicial proceedings.

For personal data that enters into the scope of application of the PDPL, the transfer, sharing, exchange or processing of personal data to a foreign country that does not provide an adequate level of protection is permitted with the explicit consent of the data subject or their legal representative, in the following cases:

- where the transfer is carried out for international judicial co-operation; or
- where the transfer or exchange is implemented pursuant to a bilateral or multilateral international agreement to which Egypt is a party.

5.5 Recent Developments

The Regulations were issued in November 2025, setting out the requirements, procedures and applicable fees for cross-border transfers of personal data. Looking ahead, the Center is expected to issue specific guidelines addressing cross-border data transfers, to further clarify the applicable requirements.



Law and Practice

Contributed by:

Charlotte Gerrish and Evane Alexandre
Gerrish Legal

Contents

1. Legal and Regulatory Framework p.88

- 1.1 Overview of Data and Privacy-Related Laws p.88
- 1.2 Rights and Obligations p.88
- 1.3 Special Categories of Personal Data p.89
- 1.4 Processing of Personal Data for Research and Development Purposes p.90
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.91
- 1.6 Data Breach Requirement p.91
- 1.7 Regulators p.92
- 1.8 Enforcement Proceedings and Fines p.93
- 1.9 Enforcement Trends p.94

2. Privacy Litigation p.95

- 2.1 Privacy Litigation Overview p.95
- 2.2 Recent Case Law p.96
- 2.3 Collective Redress Mechanisms p.97

3. Requirements for the Protection and Processing of Non-Personal Data p.97

- 3.1 Objectives and Scope of Data Regulation p.97
- 3.2 Interaction of Data Regulation and Data Protection p.98
- 3.3 Rights and Obligations Under Applicable Data Regulation p.98
- 3.4 Regulators and Enforcement p.99

4. Sectoral Topics p.99

- 4.1 Use of Cookies p.99
- 4.2 Personalised Advertising and Other Online Marketing Practices p.100
- 4.3 Employment Privacy Law p.100
- 4.4 Data Protection in M&A p.100

5. International Considerations p.101

- 5.1 Restrictions on International Data Transfers p.101
- 5.2 Government Notifications and Approvals p.101
- 5.3 Data Localisation Requirements p.101
- 5.4 Blocking Statutes p.101
- 5.5 Recent Developments p.102

Gerrish Legal is a Paris and Stockholm-based boutique law firm with additional presence in London, specialising in privacy, data protection, AI and technology law. With lawyers qualified in France, England and Wales and Ireland, the firm's multilingual team advises international clients – from scale-ups to listed multinationals – across sectors such as SaaS, life sciences, fashion, recruitment, security and catering. Its core practice focuses on GDPR compliance, international data transfers, AI regulation, digital platform regulation, privacy-by-design frameworks, data

breach management and privacy litigation. The firm also has strong expertise in commercial law, particularly technology contracts (SaaS), cross-border commercial arrangements and intellectual property matters. Gerrish Legal advises both EU-based organisations on privacy compliance and non-EU companies expanding into Europe (particularly France) by adapting their data governance frameworks and commercial practices to EU regulatory requirements, including the GDPR, AI Act, Data Act and sector-specific digital regulations.

Authors



Charlotte Gerrish is the founder of Gerrish Legal and a Franco-British lawyer qualified in France, England and Wales, Ireland, and registered with the Swedish Bar Association as an EU Lawyer. Based in Paris and

Stockholm, she specialises in privacy, data protection, AI and technology law, advising clients on GDPR compliance, international data transfers, AI regulation, privacy litigation and digital regulatory frameworks. Her practice encompasses strategic technology (SaaS) contracting, cross-border commercial arrangements and compliance advisory. Charlotte regularly assists non-EU companies expanding into France and Europe, adapting their data governance and commercial frameworks to EU regulatory requirements including the GDPR, AI Act and Data Act.



Evane Alexandre is a French-qualified lawyer admitted to the Paris Bar specialising in privacy, data protection, AI and technology law. A graduate of the DJCE Master's programme with an LLM from an

American university, she advises clients on GDPR compliance, international data transfers, AI regulation, privacy-by-design implementation and data governance frameworks. Her professional experience spans law firms, global companies and academia, including the legal department of a French luxury fashion house. At Gerrish Legal, she combines her privacy expertise with a strong foundation in French commercial and contract law, providing strategic guidance on technology agreements, cross-border data flows and regulatory compliance.

Gerrish Legal

15 rue de Surène
75008
Paris
France

Kammakargatan 47
11124
Stockholm
Sweden

Tel: +33 6 74 02 45 07
Email: info@gerrishlegal.com
Web: www.gerrishlegal.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

EU data protection law is grounded in EU constitutional sources, notably Article 16, Treaty on the Functioning of the European Union (TFEU) which constitutes the legal basis for legislation and fundamental rights protection (Article 7 of the Charter of Fundamental Rights of the EU which consecrates respect for private life and family life, and Article 8 which directly consecrates the protection of personal data). These establish both EU legislative competence and the constitutional status of data protection as a fundamental right).

The centrepiece of the data privacy framework is the General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data), which was adopted by the EU and became directly applicable across all member states on 25 May 2018 without the need for national transposition.

The GDPR prevails over incompatible national provisions. Its objective is to ensure an equal and harmonised level of protection for personal data across the Union while safeguarding the free movement of such data. It operates as the EU's general (horizontal) regime for personal data processing.

These sources interact through the primacy and direct applicability of EU law: the GDPR serves as the default framework, while sectoral instruments either displace it for specific scopes or add rules consistent with GDPR principles (*lex specialis*).

EU-level interpretation is also shaped materially by Court of Justice of the European Union (CJEU) case law. The CJEU's jurisprudence has been central in defining core concepts of data protection law.

Additionally, EU regulatory convergence is promoted through EDPB soft-law instruments (for example, Guidelines 05/2021). While formally non-binding, these guidelines play a significant harmonising role in enforcement practice.

The GDPR has explicit extraterritorial reach where processing relates to the offering of goods or services to individuals in the EU or monitoring their behaviour in the EU (Article 3 (2), GDPR), and its international transfer regime can significantly extend compliance requirements beyond the EU (Chapter V, GDPR), as reflected in leading transfer case law (CJEU, *Schrems II*, Case C-311/18).

The EU privacy/data protection framework also overlaps with EU regimes on non-personal data, cybersecurity and AI: non-personal and mixed datasets are addressed through the free flow framework and data economy rules (Regulation (EU) 2018/1807 (Free Flow of Non-Personal Data); Regulation (EU) 2022/868 (Data Governance Act); Regulation (EU) 2023/2854 (Data Act)), while security obligations intersect with GDPR security requirements (Directive (EU) 2022/2555 (NIS2 Directive); Article 32, GDPR). AI governance adds further product- and risk-based obligations that must be implemented alongside GDPR where personal data is used (Regulation (EU) 2024/1689 (AI Act)).

1.2 Rights and Obligations

Under EU law, the general principles governing the processing of personal data are set out in the GDPR.

Article 5, GDPR establishes core principles which structure all processing activities: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability (Article 5 (1)-(2), GDPR).

Chapter 2 (Articles 6-11), GDPR sets out the substantive conditions for lawful processing. Processing must be based on one of the lawful grounds listed in Article 6, GDPR (consent, contract, legal obligation, vital interests, public task or legitimate interests) (Article 6 (1), GDPR), with stricter conditions for special categories of data (Article 9, GDPR).

Chapter 4 (Articles 24-43), GDPR establishes obligations for controllers and processors.

Controllers bear primary responsibility for ensuring and demonstrating compliance (Articles 5 (2) and 24), must implement data protection by design and by default (Article 25), conduct data protection impact

assessments where processing is likely to result in high risk (Article 35), appoint a data protection officer where required (Articles 37–39) and ensure appropriate technical and organisational security measures proportionate to risk (Article 32).

Processors may process data only on documented instructions from the controller (Article 28), must implement appropriate security measures (Article 32) and assist controllers in fulfilling data subject rights and compliance duties.

Organisations acting as controllers or processors must operationalise the accountability principle (Articles 5 (2) and 24, GDPR) through documentation, internal governance structures and demonstrable risk management practices.

Chapter 3 (Articles 12–23) also grants data subjects a broad catalogue of enforceable rights. These include the right to transparent information at the time of collection (GDPR, Articles 12–13); the right of access (Article 15); rectification (Article 16); erasure (“right to be forgotten”) (Article 17); restriction of processing (Article 18); data portability (Article 20); and objection, including an absolute right to object to direct marketing (Article 21). Individuals also have rights relating to automated decision-making and profiling (Article 22). Requests must generally be answered within one month (Article 12 (3)), and data subjects may lodge complaints with a supervisory authority (Article 77) and seek judicial remedies (Articles 78–79).

The CJEU has played a central role in interpreting these rights (for example, *Google Spain*, C-131/12; *Schrems II*, C-311/18).

Key “to dos” include:

- maintaining a record of processing activities (Article 30);
- conducting data protection impact assessments where processing is likely to result in high risk (Article 35), and consulting supervisory authorities where residual high risk remains (Article 36);
- implementing appropriate technical and organisational security measures (Article 32);

- establishing procedures for detecting and managing personal data breaches, including notification within 72 hours where required (Articles 33–34);
- appointing a data protection officer where mandatory (Article 37); and
- ensuring lawful transfer mechanisms for international data flows (Chapter V GDPR).

These obligations operate cumulatively with relevant sectoral instruments such as the e-Privacy Directive (Directive 2002/58/EC) and, where applicable, Directive (EU) 2016/680.

1.3 Special Categories of Personal Data

As a principle, Article 9 (1), GDPR prohibits processing data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, health data, and data concerning sex life or sexual orientation.

By exception, such processing is permitted only where one of the exhaustively listed grounds in Article 9 (2) applies, namely:

- explicit consent (Article 9 (2)(a));
- employment, social security and social protection obligations under EU or Member State law (Article 9 (2)(b));
- vital interests (Article 9 (2)(c));
- legitimate activities of certain non-profit bodies (Article 9 (2)(d));
- data manifestly made public by the data subject (Article 9 (2)(e));
- legal claims (Article 9 (2)(f));
- substantial public interest (Article 9 (2)(g));
- preventive or occupational medicine and health care management (Article 9 (2)(h)–(3));
- public health (Article 9 (2)(i)); and
- archiving, scientific or historical research and statistical purposes subject to safeguards (Article 9 (2)(j) and Article 89 (1)).

Automated decision-making based on special categories of data is further restricted by Article 22 (4) of the GDPR. Member states may introduce additional conditions for genetic, biometric and health data (Article 9 (4), GDPR).

The GDPR also provides a specific regime for children's data in the context of information society services. Where processing is based on consent (Article 6 (1)(a), GDPR) and relates to the direct offer of such services to a child, consent is valid only if the child is at least 16 years old, unless member states lower the age threshold (not below 13) (Article 8 (1), GDPR). For children below the applicable age, consent must be given or authorised by the holder of parental responsibility, and controllers must make reasonable efforts to verify this (Article 8 (2), GDPR).

Data relating to criminal convictions, offences and related security measures are governed separately under Article 10, GDPR. Unlike Article 9 data, such data may be processed only under the control of a public authority or where authorised by EU or member state law providing appropriate safeguards.

Comprehensive registers of criminal convictions may be kept only under the control of a public authority. In the law enforcement context, processing by competent authorities falls under Directive (EU) 2016/680 (Law Enforcement Directive), which establishes a parallel regime.

1.4 Processing of Personal Data for Research and Development Purposes

Patient data is a special category of personal data under Article 9, GDPR. As a principle, processing health data is prohibited, unless an Article 6 legal basis and an Article 9 (2) exception applies.

Health data includes information relating to physical or mental health, such as healthcare services, genetic and biometric data.

Only data that is truly anonymised falls outside the GDPR. Pseudonymised data remains personal data. The processing carried out to achieve anonymisation must itself be lawful.

In practice, life sciences companies most commonly rely on:

- explicit consent (Article 9 (2)(a)), given specifically for research or product development purposes,

and provided it is explicit, freely given, specific and informed;

- scientific research purposes (Article 9 (2)(j)), provided the processing is based on EU or member state law and subject to appropriate safeguards under Article 89 (1), GDPR (eg, pseudonymisation, access controls, data minimisation);
- public interest in the area of public health (Article 9 (2)(i)), such as ensuring high standards of quality and safety of healthcare or medical devices, where supported by EU or member state law; and
- preventive or occupational medicine, diagnosis or management of healthcare systems (Article 9 (2)(h) GDPR), particularly where the company acts on behalf of or in co-operation with healthcare providers subject to professional secrecy.

The European Health Data Space Regulation (EHDS), once applicable, will significantly impact life sciences companies operating in the EU by establishing a harmonised framework for secondary use of electronic health data.

Secondary use for research, innovation, regulatory purposes and public health policy will require a data permit issued by a national health data access body. Permits will specify the authorised purpose, datasets and conditions of use, and data will generally be accessed through secure processing environments, subject to strict purpose limitation, security, governance controls and a prohibition on re-identification. The EHDS expressly prohibits certain uses (eg, advertising, discriminatory decision-making, decisions detrimental to individuals in areas such as employment or insurance).

It further strengthens individuals' rights (including enhanced access and portability, and in some cases the ability to restrict secondary use) and introduces interoperability obligations for electronic health record systems, reinforcing privacy by design under the GDPR.

Overall, the EHDS aims to facilitate innovation by expanding lawful access to large-scale health datasets while tightening governance and limiting purely commercial uses. Together, the GDPR and EHDS create a high-compliance but innovation-oriented

regime: companies may anonymise and use patient data for development or research where valid grounds exist and robust safeguards are in place, while future access will increasingly depend on EHDS governance compliance.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Under EU law, any AI system that processes personal data is subject to the GDPR. Controllers must identify a valid Article 6 legal basis (and Article 9 exception where special categories are involved), comply with the core principles in Article 5 (including fairness, transparency, purpose limitation, data minimisation and accuracy), and implement data protection by design and by default (Article 25). Given the scale and complexity of AI training and inference, Article 32 security obligations are particularly significant. A Data Protection Impact Assessment is required under Article 35 where AI processing is likely to result in a high risk, including large-scale profiling, behavioural inference or use of sensitive data.

Article 22, GDPR also specifically restricts decisions based solely on automated processing that produce legal or similarly significant effects. Such decisions are prohibited unless one of the narrow exceptions apply: necessity for entering into or performing a contract, authorisation by EU or member state law with appropriate safeguards, or explicit consent. In those cases, controllers must ensure meaningful human intervention and enable individuals to express their views and contest the decision, and must provide meaningful information about the logic involved and the envisaged consequences.

The Artificial Intelligence Act (AI Act) also established a harmonised, risk-based framework for the development, placing on the market and deployment of AI systems in the EU. It classifies systems into prohibited, high-risk, limited-risk and minimal-risk categories:

- prohibited practices (eg, certain manipulative techniques, social scoring and specific biometric identification uses) may not be deployed;
- high-risk systems, including those used in employment, creditworthiness, law enforcement, migration, education and critical infrastructure, are

subject to ex ante conformity assessments and ongoing compliance obligations;

- limited-risk systems, mainly subject to transparency obligations; and
- minimal-risk systems, which are largely unregulated under the AI Act.

For high-risk systems, the Act imposes extensive requirements centred on risk management, technical documentation, record-keeping, robustness and cybersecurity. A core focus is data governance: providers must ensure appropriate data management practices, assess the quality of training, validation and testing datasets, implement bias detection and mitigation measures, and document data sources and preprocessing methods.

Transparency is required across several risk levels. Users must be informed when interacting with an AI system (eg, chatbots) or when content is AI-generated (eg, deepfakes). High-risk systems must also be accompanied by clear instructions for use and sufficient information to enable effective oversight.

Human oversight is a structural requirement for high-risk systems: they must be designed so that natural persons can understand system capabilities and limitations, monitor outputs and intervene or override where necessary.

The regimes are complementary: the GDPR governs the lawfulness of personal data processing and individual rights, while the AI Act regulates AI systems from a product safety and governance perspective. In practice, GDPR compliance is always required where personal data is involved, and additional AI Act obligations apply depending on risk classification, with transparency, data governance and human oversight forming the core pillars for high-risk AI.

1.6 Data Breach Requirement

Under EU law, a “personal data breach” is defined as a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Article 4 (12), GDPR). This covers confidentiality breaches (unauthorised access/disclosure), availability breaches (loss/inac-

cessibility) and integrity breaches (unauthorised alteration).

Controllers and processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to risk (Articles 5 (1)(f) and 32, GDPR), adopting a risk-management approach rather than guaranteeing absolute security (eg, CJEU, *Natsionalna agentsia za prihodite*, Case C-340/21).

When a breach occurs, controllers must promptly assess whether it is likely to result in a risk to individuals' rights and freedoms, and comply with the GDPR's notification and documentation obligations.

Where the breach is likely to result in a risk, the controller must notify the competent supervisory authority without undue delay and, where feasible, within 72 hours after becoming aware of it (Article 33 (1), GDPR); any delay must be justified.

Processors must notify the controller without undue delay after becoming aware of a breach (Article 33 (2), GDPR). The notification must include, at minimum, a description of the breach, the categories and approximate number of data subjects and records concerned, contact details for the DPO or other point of contact, likely consequences and measures taken or proposed to address and mitigate the breach (Article 33 (3), GDPR); information may be provided in phases (Article 33 (4), GDPR).

Controllers must document all breaches (facts, effects, remedial action) to enable regulatory verification (Article 33 (5), GDPR). Where the breach is likely to result in a high risk, the controller must communicate it to affected individuals without undue delay, using clear and plain language and providing equivalent core information and mitigation steps (Article 34 (1)–(2), GDPR).

Communication to individuals may be avoided in limited cases, including where robust technical measures (eg, effective encryption) render the data unintelligible, or where subsequent measures eliminate the high risk, or where individual notification would involve disproportionate effort (in which case a public communication may be used) (GDPR, Article 34 (3)).

Operationally, organisations should have a breach response plan that enables rapid detection, containment and documentation; an initial legal and technical qualification of the event; a structured risk assessment; timely regulator and (if required) individual notifications; and remediation steps (containment, patching, credential resets, access reviews, restoration and enhanced monitoring), followed by a post-incident review (Articles 24, 25 and 32, GDPR).

Supervisory authorities have extensive investigative and corrective powers, including requiring information, conducting audits, ordering notifications, restricting processing and imposing administrative fines (Articles 57, 58 and 83, GDPR). However, corrective measures are not automatic and must be necessary and proportionate (see judgment of 26 September 2024 C-768/21).

Data breaches also create civil liability exposure and potential mass claims. Data subjects may lodge complaints with supervisory authorities (Article 77, GDPR) and seek judicial remedies and compensation for material or non-material damage (Articles 79 and 82, GDPR). The Court of Justice has confirmed that fear of potential misuse of data following a breach may itself constitute compensable non-material damage (*Natsionalna agentsia za prihodite*).

1.7 Regulators

At EU level, privacy and data protection oversight is organised around national supervisory authorities, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), with additional roles for sectoral regulators under specific instruments (eg, the ePrivacy Directive).

National Supervisory Authorities (NSAs)

Under Article 51, GDPR, each member state must designate at least one independent authority responsible for monitoring and enforcing the GDPR. NSAs are vested with investigative, corrective and sanctioning powers under Articles 57 and 58, GDPR, including the power to conduct audits and inspections, require information, order compliance, impose processing bans and administrative fines.

Proceedings are typically triggered by (i) complaints lodged by data subjects (Article 77, GDPR), (ii) referrals or co-operation requests from other supervisory authorities in cross-border cases, or (iii) ex officio investigations. In cross-border cases, the “one-stop-shop” mechanism (Articles 56 and 60, GDPR) designates a lead supervisory authority, which co-operates with other “concerned” authorities. Disputes may be escalated to the EDPB for a binding decision under Article 65, GDPR.

NSAs also enforce Directive 2016/680 (law enforcement data processing) and, depending on national law, the ePrivacy Directive (2002/58/EC), sometimes alongside or instead of sector-specific regulators (eg, telecommunications authorities). Their decisions are binding domestically, subject to judicial review.

European Data Protection Board (EDPB)

Established under Articles 68–76, GDPR, the EDPB ensures consistent application of the GDPR across the Union. It issues guidelines, recommendations and best practices (Article 70 GDPR), advises the European Commission (including on adequacy decisions), and adopts binding decisions in dispute resolution under Article 65. Its guidelines are formally non-binding but highly persuasive in practice; Article 65 decisions are legally binding on the national authorities concerned.

European Data Protection Supervisor (EDPS)

The EDPS supervises compliance with EU data protection rules by EU institutions, bodies and agencies (currently under Regulation (EU) 2018/1725). It exercises comparable investigative and corrective powers within the EU institutional framework and may issue reprimands, orders or administrative fines. Its decisions are binding on EU institutions and subject to review by the CJEU.

Sectoral and Related Authorities

Under the ePrivacy Directive, member states may designate specific authorities for rules on confidentiality of communications, cookies and direct marketing rules. The GDPR’s one-stop-shop mechanism does not automatically apply to national rules implementing the ePrivacy Directive, which may lead to parallel national proceedings.

In addition, for international data transfers, the European Commission plays a key role through adequacy decisions (Article 45, GDPR), while national authorities retain investigative powers and may refer validity questions to the CJEU (as illustrated by *Schrems* case law).

1.8 Enforcement Proceedings and Fines

Under EU law, investigations and enforcement actions in data protection matters are primarily governed by the GDPR, which establishes a decentralised enforcement system based on independent national supervisory authorities (Articles 51–59, GDPR), combined with a co-operation and consistency mechanism for cross-border processing (Articles 56, 60–66, GDPR).

Initiation of Investigations

Proceedings may be triggered by (i) a complaint lodged by a data subject (Article 77, GDPR), (ii) ex officio action by a NSA, or (iii) a co-operation request from other supervisory authorities in cross-border cases (Articles 60–61, GDPR). In cross-border scenarios, the “lead supervisory authority” (usually that of the controller’s main establishment) conducts the investigation under the one-stop-shop mechanism (Article 56, GDPR), in co-operation with “concerned” authorities. If disagreement persists, the matter may be referred to the EDPB, which can adopt a binding decision under the consistency mechanism (Article 65, GDPR).

Conduct of Investigations and Procedural Guarantees

NSAs have extensive investigative powers, including the power to order the provision of information, carry out audits and inspections, and access to premises and data (Article 58 (1), GDPR). They may adopt corrective measures (Article 58 (2) GDPR), including warnings, reprimands, orders to comply, temporary or definitive processing bans, suspension of data flows and administrative fines.

The GDPR does not fully harmonise procedural timelines for investigations; these are governed by national administrative law, subject to EU law principles of effectiveness, equivalence and the right to good administration (Article 41, Charter of Fundamental Rights of the EU) and the right to an effective remedy

(Article 47, Charter). Data subjects must be informed of the progress or outcome of their complaint and have the right to challenge legally binding decisions or inaction before national courts (Articles 78–79, GDPR).

Controllers must respond to data subject requests within one month, extendable by two further months where necessary (Article 12 (3), GDPR). Failure to respond may prompt a complaint and subsequent enforcement. In practice, national laws may provide for hearings, written submissions and settlement-like discussions during investigations, but there is no harmonised EU-level “transaction” mechanism; informal resolution or commitments may nevertheless influence the authority’s choice of corrective measures.

Sanctions and Remedies

The GDPR provides for a harmonised regime of administrative fines (Article 83, GDPR), structured in two tiers: up to EUR10 million or 2% of the total worldwide annual turnover (Article 83 (4)), and up to EUR20 million or 4% of worldwide annual turnover (Article 83 (5)), whichever is higher. Fines must be effective, proportionate and dissuasive (Article 83 (1)). In addition, supervisory authorities may impose non-pecuniary corrective measures (Article 58 (2)). Member states may lay down additional penalties, including criminal sanctions, for infringements not subject to administrative fines or to supplement them (Article 84).

Data subjects are entitled to compensation for material or non-material damage resulting from a GDPR infringement (Article 82). Controllers and processors may be held jointly and severally liable, subject to rights of recourse between them.

Criteria for Setting Penalties

Article 83 (2), GDPR lists the factors to be taken into account when deciding whether to impose a fine and determining its amount. These include: the nature, gravity and duration of the infringement; the number of data subjects affected and the level of damage; whether the infringement was intentional or negligent; actions taken to mitigate damage; the degree of responsibility, taking into account technical and organisational measures; previous infringements; co-operation with the authority; categories of personal data involved; how the infringement became

known; compliance with prior measures; adherence to approved codes of conduct or certification mechanisms; and any financial benefits gained or losses avoided.

Recent CJEU case law (eg, Joined Cases C-683/21 and C-807/21, 5 December 2023) confirms that administrative fines require a culpable infringement (intentional or negligent conduct) attributable to the controller or processor.

Overall, EU enforcement combines harmonised substantive with national procedural frameworks. The system is designed to ensure consistent application across the Union, while preserving judicial oversight by national courts and, ultimately, the CJEU.

1.9 Enforcement Trends

In the last 24 months, EU enforcement has centred on the accountability principle. National supervisory authorities and the CJEU increasingly require operational compliance frameworks, not merely formal documentation.

Accountability, Automated Decision-Making and Minimisation

Recent CJEU case law has clarified fault requirements for administrative fines in *Deutsche Wohnen* (C-807/21) and *National Police of Latvia* (C-683/21), strictly interpreted the prohibition on automated decision-making in *SCHUFA* (C-634/21), and reinforced data minimisation and purpose limitation in *Schrems v Meta* (C-446/21). In its 4 October 2024 judgment in *Schrems v Meta* (C-446/21), the court held that large-scale, indefinite processing for behavioural advertising cannot be justified simply because some data was made public. Together, these rulings confirm that accountability and privacy by design/default (Articles 24–25 GDPR) are concrete, documented governance obligations.

Practical takeaway

GDPR compliance must function as embedded, risk-based governance infrastructure, evidenced in practice.

International Data Transfers

After the CJEU invalidated *Safe Harbor* and *Privacy Shield* in *Schrems* (C-362/14) and *Schrems II* (C-311/18), the Commission adopted the EU-US Data Privacy Framework (Implementing Decision (EU) 2023/1795). In *Latombe v Commission* (T-553/23, 3 September 2025), the General Court upheld the adequacy decision, accepting that safeguards introduced by Executive Order 14086 and the Data Protection Review Court could ensure essentially equivalent protection.

The EDPB's Guidelines 05/2021 (adopted 14 February 2023) clarified the cumulative criteria for a "transfer" under Chapter V, GDPR. Concurrently, CJEU case law has reaffirmed that supervisory authorities retain investigative powers even where an adequacy decision exists, consistent with *Schrems II*.

Practical takeaway

Organisations should map cross-border data flows, rely on adequacy decisions where available, conduct and document transfer impact assessments for non-adequate destinations, and periodically reassess transfers – even where DPF certification applies.

Security, Liability and Regulatory Convergence

In *Natsionalna agentsia za prihodite* (C-340/21), the CJEU confirmed that fear of misuse after a breach may constitute compensable non-material damage under Article 82 GDPR, increasing litigation exposure. In *IAB Europe* (C-604/22), the court adopted a broad approach to joint controllership in digital advertising, while in *EDPS v SRB* (C-413/23 P) it emphasised contextual identifiability in assessing pseudonymised data.

Parallel obligations under the Digital Services Act (Regulation (EU) 2022/2065) and the Data Act (Regulation (EU) 2023/2854, applicable from 12 September 2025) reinforce convergence.

Practical takeaway

Organisations should implement integrated compliance models aligning GDPR governance with platform, advertising and data-sharing obligations.

Overall, enforcement reflects a fundamental-rights-oriented, proportionate and evidence-based standard: demonstrable, risk-based compliance embedded in organisational decision-making.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Mass and Collective Data Privacy Actions

A defining trend is the growth of mass claims, particularly in jurisdictions with procedural mechanisms facilitating collective redress (eg, the Netherlands), and member states implementing the Representative Actions Directive (EU) 2020/1828). These mechanisms lower procedural barriers and increase strategic litigation risk for large-scale data processing operations.

Damages

Courts across Europe are seeing a rise in compensation claims under Article 82, GDPR, especially for non-material damages – one of the most debated issues in EU data protection law. A central question is whether "loss of control" over personal data is sufficient to establish damage. The CJEU clarified in *UI v Österreichische Post AG* (C-300/21, 4 May 2023) that mere infringement of the GDPR is not sufficient: claimants must demonstrate actual damage and a causal link, although no minimum seriousness threshold is required. This leaves national courts discretion in interpreting and quantifying non-material harm.

Security

Beyond classic post-breach litigation, claims increasingly scrutinise the adequacy of technical and organisational measures under Article 32, GDPR, as well as incident detection and notification practices under Articles 33-34. In *Natsionalna agentsia za prihodite* (C-340/21), the CJEU confirmed that the mere occurrence of a breach does not automatically establish non-compliance; courts must assess whether the security measures implemented were appropriate to the risk.

International Data Transfers

Cross-border data transfers remain a significant source of litigation and regulatory exposure. Organisations must navigate adequacy decisions, standard

contractual clauses and politically contested frameworks such as the EU–US Data Privacy Framework, which continues to attract scrutiny from privacy activists and regulators. Transfer impact assessments and ongoing monitoring remain essential in practice.

Technology-Driven Disputes

A growing strand of litigation and regulatory action concerns technology-driven processing, particularly where AI, automated profiling and other high-risk algorithmic systems intersect with data protection rights. Regulatory investigations into AI chatbots generating deepfake or harmful content illustrate heightened scrutiny of system design, risk assessments and compliance with GDPR obligations, especially where sensitive data or children’s rights are implicated.

Disputes also arise from large-scale biometric and tracking practices, underscoring continued regulatory focus on facial recognition and mass surveillance technologies.

2.2 Recent Case Law

At EU level, in the past two years, the CJEU has delivered a series of judgments that have significantly structured privacy litigation in the EU, particularly in relation to Article 82, GDPR compensation claims, security obligations and the scope of data subject rights. Many of these decisions refine and consolidate an increasingly coherent line of case law governing civil liability and procedural standards in GDPR litigation.

- Compensation under Article 82, GDPR – in *Österreichische Post* (C-300/21, 4 May 2023), the court clarified that compensation requires three cumulative elements: (i) an infringement of the GDPR, (ii) actual damage (material or non-material), and (iii) a causal link between the infringement and the damage. A mere infringement is insufficient to found liability. At the same time, member states may not impose a minimum seriousness threshold for non-material damage. The judgment firmly established Article 82 as a compensatory (not punitive) mechanism and structured the analytical framework now applied by national courts.
- Security obligations and breach-related liability (Articles 24 and 32 GDPR) – in *Natsionalna agent-*

sia za prihodit (C-340/21, 14 December 2023), the court clarified that the mere occurrence of unauthorised disclosure or access does not automatically establish that the controller failed to implement “appropriate” technical and organisational measures under Articles 24 and 32, GDPR. The appropriateness of security measures must be assessed concretely and in light of the risk, taking into account the nature of the processing and the data involved. The CJEU thus rejected any irrebuttable presumption that a breach equals non-compliance. However, it acknowledged that erroneous disclosure by employees may indicate deficiencies in organisational measures if it reflects inadequate risk assessment or internal governance. The judgment also confirmed that fear of misuse may constitute non-material damage, provided that it is well founded and substantiated. This case therefore reinforces the risk-based logic of the GDPR while maintaining a fact-sensitive approach to liability.

- Fear, loss of control and hypothetical risk (Article 82) – in *MediaMarktSaturn* (C-687/21, 25 January 2024), the CJEU further clarified the boundaries of non-material damage. It held that the concept of “non-material damage” may, in principle, encompass well-founded fear of future misuse and even temporary loss of control over personal data. However, a purely hypothetical risk is insufficient. Where it is established that an unauthorised third party did not actually become aware of the personal data, the mere fear of possible future dissemination does not, in itself, constitute compensable damage. The judgment reiterates that the data subject must demonstrate actual damage, however minimal. In this respect, *MediaMarktSaturn* does not depart from earlier case law but refines it by drawing a clearer distinction between abstract risk and substantiated harm.
- Liability regime and burden of proof (Article 82 (3)) – in *juris GmbH* (C-741/21, 11 April 2024), the CJEU clarified the operation of Article 82 (3), confirming that the GDPR establishes a fault-based liability regime with a reversed burden of proof. A controller cannot avoid liability merely by arguing that the damage resulted from negligence of an employee acting under its authority. Since employees act under the controller’s authority within the meaning of Article 29, GDPR, the controller

remains responsible unless it proves that it was not in any way responsible for the event giving rise to the damage. The exemption under Article 82 (3) therefore applies only where the controller demonstrates the absence of a causal link.

- Right of access and scope of the “copy” obligation (Article 15 GDPR) – in *FT v DW* (C-307/22, 26 October 2023), the CJEU strengthened the effectiveness of the right of access. It held that patients are entitled to obtain a first copy of their medical records free of charge, irrespective of the purpose of the request, including where the data is sought for potential litigation. National law cannot impose systematic fees for the first copy. The CJEU also clarified that the right to obtain a “copy” may require full reproduction of documents, including diagnoses and treatment details, where necessary to ensure intelligibility and effective exercise of rights.

Taken together, these decisions have not revolutionised EU privacy litigation but have consolidated a structured and increasingly predictable framework. This jurisprudence now provides national courts with a coherent template for adjudicating GDPR-based civil claims.

2.3 Collective Redress Mechanisms

At EU level, collective redress in privacy and data protection matters is structured around Article 80, GDPR and the Representative Actions Directive (RAD) (Directive (EU) 2020/1828).

Article 80, GDPR allows not-for-profit organisations representing data subjects to bring complaints and judicial remedies on their behalf. Member states may also permit such organisations to act without an individual mandate. This mechanism has enabled strategic litigation by consumer and privacy associations, particularly in cases involving large-scale tracking, platform practices and data breaches.

The RAD, applicable since 25 June 2023, requires all member states to ensure the availability of representative actions aimed at protecting the collective interests of consumers. It applies to infringements of a broad list of EU legislation set out in Annex I, including data protection rules.

Only designated “qualified entities” may bring representative actions under the RAD. These must generally be non-profit organisations or public bodies pursuing consumer interests and satisfying independence and transparency requirements, including safeguards regarding third-party funding. For cross-border actions, designation criteria are harmonised and subject to mutual recognition across member states.

The RAD requires member states to provide for both injunctive measures and redress measures (including compensation), but it leaves significant procedural discretion at national level. In particular, member states may choose between opt-in or opt-out participation models, or adopt hybrid approaches, especially for redress actions. As a result, the structure and practical reach of collective compensation vary across jurisdictions.

Participation models (opt-in or opt-out) and the availability of collective compensation therefore differ across member states. In practice, injunctions remain more common and procedurally straightforward than collective damages. Recent developments centre on the domestic implementation of the RAD and the gradual emergence of case law applying these new mechanisms, with some jurisdictions (notably the Netherlands and Germany) becoming more active fora for data-related collective litigation.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

At EU level, rules on non-personal data are shaped primarily by a set of “data economy” instruments to facilitate data circulation, access and market fairness, rather than solely protect privacy.

The Free Flow of Non-Personal Data Regulation (Regulation (EU) 2018/1807) addresses barriers to the movement of non-personal data within the internal market by prohibiting member states from enforcing data localisation restrictions for non-personal data, allowing it to be stored or processed anywhere in the EU.

The Data Governance Act (Regulation (EU) 2022/868) complements this framework by creating mechanisms to encourage voluntary data sharing. It regulates data intermediation services, introduces a framework for data altruism organisations, and establishes conditions for the reuse of certain protected public sector data.

The Data Act (Regulation (EU) 2023/2854) goes further and provides a broad, cross-sector regime governing access to and use of data generated by connected products and related services, including in the IoT environment. It imposes obligations on data holders to make data available to users and, in defined circumstances, to third parties. It also introduces business-to-business data sharing obligations subject to fair, reasonable and non-discriminatory (FRAND) conditions, establishes rules to facilitate cloud switching and interoperability, and includes safeguards against unlawful access by third-country authorities.

Taken together, these instruments form a layered regulatory architecture in which non-personal data regulation, competition policy and data protection law operate in parallel and, where relevant, cumulatively.

3.2 Interaction of Data Regulation and Data Protection

The EU's data economy instruments are designed to operate alongside, not instead of, the GDPR. They regulate access to and use of data, but do not alter the fundamental rules governing the processing of personal data.

Where datasets are purely non-personal, instruments such as the Free Flow of Non-Personal Data Regulation and the Data Act apply without triggering GDPR obligations. In the case of mixed datasets, the GDPR continues to govern the personal data component, while the data economy framework regulates access, sharing and portability at the level of the dataset.

The Data Act expressly states that it does not affect the application of Union data protection law. Accordingly, any data-sharing obligation must comply with GDPR requirements, including the existence of a lawful basis, respect for purpose limitation and data minimisation, and appropriate security safeguards.

Non-personal data may also be protected under trade secret law, intellectual property rules or contractual confidentiality. The Data Act seeks to balance broader access rights with the protection of commercially sensitive information through confidentiality safeguards.

In this way, the EU framework is layered: data economy legislation promotes access and re-use, while data protection law continues to constrain the processing of personal data.

3.3 Rights and Obligations Under Applicable Data Regulation

Across the EU data economy framework, several recurring principles and obligations emerge, distributed across different instruments (Free Flow Regulation, Data Governance Act, Data Act, etc).

Common Structural Features

Although the relevant rules are spread across several instruments, they reflect a shared policy orientation. The EU data framework seeks to promote data mobility and access, reduce structural imbalances in data-driven markets, and prevent technical or contractual lock-in, while preserving confidentiality and legitimate commercial interests.

A first recurring principle is the free circulation of non-personal data within the internal market. The Free Flow Regulation prohibits unjustified data localisation requirements and reinforces the idea that non-personal data may be stored and processed anywhere in the Union.

A second core feature is the promotion of access to and re-use of data. The Data Act establishes access rights in defined contexts, particularly for data generated by connected products and related services, allowing users to obtain and, in certain cases, direct the sharing of such data with third parties. More broadly, EU legislation aims to ensure that data access is not unreasonably withheld where it is economically and socially valuable.

Fairness and non-discrimination are also central themes. In business-to-business settings, data sharing may be subject to fair, reasonable and non-discriminatory (FRAND) conditions. Switching and inter-

operability obligations for data processing services aim to prevent lock-in and enhance market contestability.

Finally, all instruments recognise the need to safeguard confidential business information. Trade secrets and commercially sensitive data remain protected, and access obligations must be implemented with appropriate confidentiality safeguards.

Instrument-Specific Rights and Duties

While these principles are common across the framework, certain instruments introduce more specific obligations.

For instance, the Data Act imposes duties on “data holders” to make product-generated data accessible to users and, in defined circumstances, to third parties. It also introduces interoperability and switching obligations for data processing service providers.

Similarly, the Data Governance Act regulates data intermediation services and data altruism organisations, requiring neutrality, transparency and organisational safeguards.

Organisational Compliance Considerations

For organisations, compliance begins with identifying their role under the relevant instruments (data holder, user, intermediary or cloud service provider) and mapping relevant data flows, particularly in IoT environments.

Contractual arrangements must be reviewed to ensure alignment with access and FRAND standards, and technical systems assessed for interoperability and switching readiness. Internal processes should safeguard trade secrets and commercially sensitive information.

Where personal data is involved, GDPR obligations apply in parallel.

3.4 Regulators and Enforcement

Under the Data Governance Act and the Data Act, member states are required to designate one or more competent authorities responsible for supervision and

enforcement. The institutional choice is left to national law, and approaches differ across the EU.

Some member states have opted to entrust enforcement, at least in part, to their data protection authority, particularly where Data Act obligations overlap with personal data processing (eg, France, Spain). Others have designated digital, communications or competition regulators as lead authorities, reflecting the market-regulatory dimension of the framework (eg, Germany, Netherlands).

This divergence reflects the hybrid nature of EU data economy legislation, which combines elements of data governance, digital market regulation and, in certain cases, competition oversight. Where personal data is involved, co-ordination with GDPR supervisory authorities is necessary. In parallel, disputes involving dominant platforms or data access conditions may also fall within the remit of competition authorities.

Overall, enforcement remains decentralised but increasingly requires co-operation across regulatory domains, mirroring the integrated structure of the EU’s digital regulatory strategy.

4. Sectoral Topics

4.1 Use of Cookies

Online tracking technologies (including cookies, SDKs, pixels and similar device identifiers) are governed primarily by Article 5 (3) of the ePrivacy Directive (Directive 2002/58/EC), as implemented in national law, in conjunction with the GDPR.

Article 5 (3) establishes a general opt-in model: storing or accessing information on a user’s device requires prior informed consent, unless the technology is strictly necessary to provide a service explicitly requested by the user. This rule applies regardless of whether the data accessed is personal data. Where personal data is subsequently processed, the GDPR applies in parallel.

Although the core consent requirement is harmonised, implementation and enforcement vary across member states. In practice, most member states require

granular, prior consent for analytics and advertising cookies, typically via consent management platforms. Legitimate interests cannot substitute for consent at the device-access stage under Article 5 (3), even if they may be relied upon for subsequent processing under the GDPR in limited contexts.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised and targeted advertising in the EU is regulated primarily under the GDPR and the ePrivacy Directive, supplemented, in the case of large online platforms, by the Digital Services Act (DSA).

Under the GDPR, personalised advertising must rely on a valid lawful basis under Article 6 and comply with transparency, purpose limitation and data minimisation principles. In practice, consent is frequently relied upon in online advertising environments, particularly where advertising is based on user-level data. The use of special categories of data for marketing purposes is generally prohibited unless explicit consent is obtained.

The DSA introduces additional constraints for online platforms, notably prohibiting targeted advertising based on profiling using sensitive data and restricting targeted advertising directed at minors based on profiling.

Rules governing unsolicited electronic marketing (such as email or SMS campaigns) derive from the ePrivacy Directive as implemented in national law. While most member states apply an opt-in model for business-to-consumer (B2C) communications, the treatment of business-to-business (B2B) marketing varies. Some jurisdictions extend consent requirements to communications addressed to corporate contacts, whereas others allow opt-out systems for professional communications, subject to national conditions.

Accordingly, although the core data protection standards applicable to personalised advertising are harmonised, practical compliance in online marketing remains partly dependent on national implementation choices.

4.3 Employment Privacy Law

In the employment context, the GDPR applies as a baseline, but Article 88 permits member states to adopt more specific workplace rules. As a result, data protection obligations are often complemented by national labour laws, works council rights or collective agreements.

Employee monitoring, whether through time-recording systems, IT usage controls or CCTV, must be justified, proportionate and transparent. Employers commonly rely on legitimate interests, but this requires a careful balancing exercise given the imbalance of power in employment relationships. Consent is generally not considered freely given in this setting.

Remote work and bring-your-own-device (BYOD) arrangements require appropriate technical and organisational measures, particularly to ensure data security and a clear separation between professional and private information.

In recruitment, processing must be limited to what is necessary for the role. Special categories of data require a specific legal basis, and information relating to unsuccessful applicants should not be retained longer than necessary.

In many member states, national labour law imposes additional safeguards, especially regarding workplace surveillance.

4.4 Data Protection in M&A

During due diligence throughout an M&A transaction, any personal data disclosed to potential buyers must be limited to what is necessary and proportionate. In practice, secure and access-restricted virtual data rooms (VDRs) are used, with encryption, logging and tiered access controls. Sensitive information should be anonymised or redacted where feasible. Disclosure must rely on a lawful basis, typically legitimate interests, and be supported by appropriate confidentiality arrangements, including NDAs and documented access restrictions.

In asset deals, the transfer of personal data to the purchaser requires a lawful basis and must remain compatible with the original purposes of processing.

Where a new controller is introduced, transparency obligations under Articles 13 and 14, GDPR may apply. In share deals, although the legal entity remains unchanged, changes in processing practices or governance structures may trigger updated transparency or internal compliance measures.

Cross-border transactions must comply with the international transfer regime under Chapter V GDPR.

Following closing, integration requires alignment of privacy notices, retention schedules and technical and organisational measures. Data must be securely transferred, retained or deleted in accordance with the agreed transaction structure and GDPR principles.

5. International Considerations

5.1 Restrictions on International Data Transfers

Cross-border transfers of personal data from the EU are governed by Chapter 5 of the GDPR.

A “transfer” occurs where personal data is disclosed or made accessible to a controller or processor in a third country (that is to say, outside of the EU) or to an international organisation. This includes remote access from outside the EU.

Personal data may be transferred to a third country only if Chapter 5 conditions are met. The primary route is an adequacy decision under Article 45, GDPR. Where the European Commission has determined that a third country ensures an essentially equivalent level of protection, personal data may flow to that country without additional transfer authorisation. In the absence of adequacy, transfers must rely on appropriate safeguards under Article 46, GDPR, most commonly standard contractual clauses or binding corporate rules. Exporters are required to assess whether the legal framework of the recipient country allows the safeguards to be effective in practice.

Derogations under Article 49, GDPR are available only for specific and occasional situations and cannot be used for systematic or large-scale transfers.

Regarding non-personal data, EU law does not impose a comparable transfer regime. However, the Data Act introduces safeguards aimed at preventing unlawful third-country governmental access to data held by EU data processing service providers.

5.2 Government Notifications and Approvals

Under the GDPR, international transfers of personal data do not generally require prior registration, notification or approval by a supervisory authority, provided that a recognised transfer mechanism under Chapter 5 is used.

Sector-specific frameworks (eg, in financial services, telecommunications or export-controlled industries) may impose separate notification or approval requirements under national or EU law.

5.3 Data Localisation Requirements

EU law promotes the free movement of data within the Union. The Free Flow Regulation prohibits member states from imposing unjustified localisation requirements for non-personal data. For personal data, the GDPR does not impose localisation requirements but restricts transfers to third countries unless Chapter V conditions are met. Remote access from a third country is typically considered a transfer and must comply with GDPR transfer mechanisms.

Sector-specific rules may impose localisation or residency requirements in limited contexts (eg, certain public sector like health or financial data), but these are exceptions rather than the rule at EU level.

5.4 Blocking Statutes

EU law contains rules that may restrict compliance with certain foreign disclosure or discovery orders.

Under Article 48, GDPR, judgments or administrative decisions from third-country authorities requiring the transfer or disclosure of personal data are enforceable in the EU only if based on an international agreement, such as a mutual legal assistance treaty (MLAT). In other words, foreign court orders cannot, by themselves, justify a transfer of personal data from the EU.

Where a foreign authority requests access to personal data, the disclosure must still comply with the applica-

ble transfer mechanism (eg, adequacy or appropriate safeguards).

5.5 Recent Developments

Recent developments at the EU level regarding the regulation of international transfers of personal data continue to be shaped by the aftermath of the judgment in *Schrems II* (C-311/18). The EU–US Data Privacy Framework (DPF) was adopted on 10 July 2023, to restore a formal transatlantic data transfer mechanism by addressing privacy concerns related to US surveillance and redress options.

Although debate persists as to whether the DPF fully achieves its intended level of protection, the General Court, in its judgment of 3 September 2025, *Latombe v Commission* (T-553/23), upheld the DPF, accepting that safeguards introduced by US Executive Order 14086 (7 October 2022) and the Data Protection Review Court could ensure a level of protection essentially equivalent to that guaranteed by EU law.

In May 2025, the Irish Data Protection Commission (DPC) imposed a substantial EUR530 million fine on TikTok Technology Limited (“TikTok”) for failing to ensure equivalent protection for personal data transferred to China. The DPC found that, despite conducting a transfer impact assessment (TIA), TikTok had not sufficiently assessed Chinese laws and practices affecting the data and therefore failed to demonstrate “essential equivalence” under the GDPR. This decision raises doubts about the sufficiency of standard contractual clauses (SCCs) for transfers to certain third countries and highlights the practical challenges of compliance where risk assessments depend on third-country legal frameworks rather than solely on the physical location of data.

The CJEU and the EDPB have also provided important clarifications on international transfer rules, including the requirement to conduct transfer impact assessments to determine whether supplementary measures are needed in addition to SCCs (see EDPB Guidelines 05/2021 and Recommendations 01/2020; *Schrems I* (C-362/14); *Schrems II* (C-311/18); *Ministerstvo zdravotníctví* (C-710/23); and *Bindl v Commission* (T-354/22)). Together, this case law and regulatory guidance consolidate a framework that requires exporters to assess third-country laws carefully and implement effective supplementary safeguards where necessary.

Looking ahead, proposed amendments under the Digital Omnibus Regulation include a more contextual definition of personal data, under which information would not qualify as personal data for a given entity if that entity cannot reasonably identify the data subject. This could potentially reduce the scope of GDPR obligations, including those related to international transfers, by excluding certain data from being classified as personal data. In practice, this may ease burdens on certain cross-border data routing arrangements by limiting the application of Chapter 5, GDPR.

In *EDPS v SRB* (C-413/23 P), the CJEU confirmed that whether information constitutes personal data depends on the circumstances, particularly on who holds the additional information necessary for re-identification and whether re-identification is reasonably likely in relation to a particular recipient. This confirms a contextual (or relational) understanding of personal data: information may constitute personal data in the hands of one actor, yet not for another recipient lacking reasonably available means of re-identification.

Trends and Developments

Contributed by:

Charlotte Gerrish and Evane Alexandre
Gerrish Legal

Gerrish Legal is a Paris and Stockholm-based boutique law firm with additional presence in London, specialising in privacy, data protection, AI and technology law. With lawyers qualified in France, England and Wales and Ireland, the firm's multilingual team advises international clients – from scale-ups to listed multinationals – across sectors such as SaaS, life sciences, fashion, recruitment, security and catering. Its core practice focuses on GDPR compliance, international data transfers, AI regulation, digital platform regulation, privacy-by-design frameworks, data

breach management and privacy litigation. The firm also has strong expertise in commercial law, particularly technology contracts (SaaS), cross-border commercial arrangements and intellectual property matters. Gerrish Legal advises both EU-based organisations on privacy compliance and non-EU companies expanding into Europe (particularly France) by adapting their data governance frameworks and commercial practices to EU regulatory requirements, including the GDPR, AI Act, Data Act and sector-specific digital regulations.

Authors



Charlotte Gerrish is the founder of Gerrish Legal and a Franco-British lawyer qualified in France, England and Wales, Ireland, and registered with the Swedish Bar Association as an EU Lawyer. Based in Paris and

Stockholm, she specialises in privacy, data protection, AI and technology law, advising clients on GDPR compliance, international data transfers, AI regulation, privacy litigation and digital regulatory frameworks. Her practice encompasses strategic technology (SaaS) contracting, cross-border commercial arrangements and compliance advisory. Charlotte regularly assists non-EU companies expanding into France and Europe, adapting their data governance and commercial frameworks to EU regulatory requirements including the GDPR, AI Act and Data Act.



Evane Alexandre is a French-qualified lawyer admitted to the Paris Bar specialising in privacy, data protection, AI and technology law. A graduate of the DJCE Master's programme with an LLM from an

American university, she advises clients on GDPR compliance, international data transfers, AI regulation, privacy-by-design implementation and data governance frameworks. Her professional experience spans law firms, global companies and academia, including the legal department of a French luxury fashion house. At Gerrish Legal, she combines her privacy expertise with a strong foundation in French commercial and contract law, providing strategic guidance on technology agreements, cross-border data flows and regulatory compliance.

Gerrish Legal

15 rue de Surène
75008
Paris
France

Kammakargatan 47
11124
Stockholm
Sweden

Tel: +33 6 74 02 45 07
Email: info@gerrishlegal.com
Web: www.gerrishlegal.com



AI Governance in 2026: Why the GDPR Remains at the Centre of Europe's Expanding Digital Rulebook *Regulatory layering, constitutional anchoring and procedural recalibration*

For US and other non-European SaaS and technology companies operating or expanding in Europe, the regulatory landscape has evolved from regulatory fragmentation into structured constitutional layering. In particular, the adoption of the Artificial Intelligence Act (Regulation (EU) 2024/1689) (AI Act) and the Data Act (Regulation (EU) 2023/2854) (Data Act) has significantly expanded the EU's digital rulebook.

Notwithstanding the breadth of these legislative developments, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) remains the central legal instrument governing AI systems whenever personal data is involved.

This centrality is neither accidental nor transitional. The AI Act expressly preserves European data protection law. The Data Act operates alongside it. More fundamentally, the GDPR's architecture is anchored in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, which the Court of Justice of the European Union (CJEU) has repeatedly interpreted as requiring effective, not merely formal, protection (see *Schrems I*, Case C-362/14; *Schrems II*, Case C-311/18). AI regulation in Europe therefore sits within an already constitutionalised data protection framework.

That constitutional positioning has concrete jurisdictional consequences. The GDPR's extraterritorial scope under Article 3 (2) ensures that non-EU controllers and processors offering goods or services to individuals in the EU, or monitoring their behaviour, fall within scope irrespective of establishment. For US and other non-European SaaS providers deploying AI-enabled analytics, behavioural optimisation tools, AI agents or foundation models into the European market, this threshold is routinely met in practice.

In practice, regulatory scrutiny of AI systems continues to crystallise through core GDPR provisions: lawful basis (Article 6), purpose limitation and minimisation (Article 5), automated decision-making safeguards (Article 22), security obligations (Article 32) and inter-

national transfer restrictions (Articles 44–49). While the AI Act introduces system-level risk categorisation and conformity assessments, those mechanisms do not displace the GDPR's operative requirements where personal data is processed. The assessment of lawfulness, proportionality and individual rights remains anchored in the GDPR.

The European Commission's publication of COM (2025) 837 final, referred to as the "Digital Omnibus", marks the first substantive legislative proposal to revisit aspects of the GDPR since 2018. It reflects an institutional recognition that the cumulative expansion of the Union's digital regulatory framework – including the AI Act, the Data Act, the DMA, the DSA and cybersecurity instruments – may generate procedural duplication and compliance friction.

However, the proposal does not alter the substantive architecture of the GDPR, nor its rights-based core. Articles 5 (principles), 6 (lawfulness), 22 (automated decision-making), 25 (protection by design), 32 (security) and Chapter V (international transfers) remain intact. Nor does it displace the jurisprudential trajectory established in *Schrems II* (Case C-311/18), *Meta Platforms* (Case C-252/21), or *SCHUFA* (Case C-634/21), each of which reinforces substantive fundamental rights protection over formalistic compliance.

For all technology companies operating or scaling in the EU, the practical conclusion is clear: Europe is refining procedural mechanics, not retreating from constitutional data governance. In 2026, the GDPR continues to constitute the primary normative and interpretative framework through which AI systems involving personal data are assessed.

From generative AI to autonomous agents at enterprise level

The technological evolution since 2023 has shifted enterprise deployment from generative output tools to agentic execution systems. AI agents increasingly perform operational functions: executing transactions, allocating resources, adjusting pricing, scoring performance, approving access and managing workflow orchestration across enterprise environments.

This shift unfolds within an expanding Union regulatory framework. The AI Act subjects certain decision-making systems to enhanced governance where they qualify as “high risk”, including systems used in creditworthiness assessments, employment, access to essential services and other consequential contexts. Such systems are subject to structured obligations relating to risk management, technical documentation, data governance and human oversight.

However, the growing operational autonomy of enterprise AI systems materially heightens exposure under Article 22 (1) GDPR, which grants individuals the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects without human intervention. The qualification of a system as “high-risk” under the AI Act does not exhaust the legal analysis. Article 22 operates independently and may apply irrespective of AI Act classification.

Article 22 was historically under-litigated. That position shifted with *SCHUFA* (Case C-634/21), where the CJEU adopted a functional approach, holding that automated credit scoring which plays a decisive role in lending decisions may fall within Article 22. The Court emphasised the real influence of algorithmic outputs, rather than the formal allocation of final decision-making authority. The inquiry thus focused on practical effect.

This reasoning is directly relevant to contemporary enterprise AI agents. Systems determining eligibility thresholds, dynamic pricing parameters, workforce scoring, procurement prioritisation or access controls may, depending on their operational influence, fall within Article 22 even where nominal human validation exists. Supervisory authorities increasingly assess whether human oversight is meaningful in substance. A nominal “human in the loop” who routinely validates automated outputs without critical review may not prevent classification as solely automated processing: the assessment is functional rather than merely formal.

At the same time, the enterprise deployment of AI agents now extends beyond clearly “decisional” systems. In commercial contexts, AI agents increas-

ingly generate tailored proposals, negotiate pricing structures and conclude transactions through conversational interfaces. In some sectors, agent-based interaction is beginning to displace traditional web infrastructure: users interact with agents that access structured datasets and generate executable outputs, with transactional completion occurring within the interface itself. In these models, the website becomes secondary; the dataset and agent architecture become primary.

Many such systems may fall outside the strict scope of Article 22 where outputs are advisory, iterative or optimisation-driven rather than determinative of legal rights. Yet this does not remove them from the GDPR framework. Where personal data is processed, the core principles of Articles 5 and 6 remain fully engaged. The compliance analysis shifts from decisional effect to structural processing risks.

In agent-based architectures, particular attention must be paid to data minimisation in large-scale ingestion models; purpose limitation where datasets are repurposed across agentic workflows; transparency obligations where decision logic is mediated through conversational interfaces rather than static disclosures; and accuracy where systems dynamically update or synthesise data in real time. The increasing autonomy of enterprise AI heightens exposure not solely because Article 22 is triggered, but because processing becomes persistent, embedded and opaque within organisational infrastructure.

The result is a layered regulatory interaction. The AI Act structures governance at the level of system design and risk categorisation. Article 22 GDPR operates as a rights-based constraint where automated outputs materially affect individuals. Beyond Article 22, the broader GDPR principles continue to regulate the scale, architecture and accountability of enterprise AI systems. Compliance with one regime does not displace the other. Enterprise AI governance therefore requires simultaneous attention to decisional effects, structural data flows and architectural autonomy.

Lawfulness, purpose limitation and continuous model optimisation

AI-driven SaaS platforms frequently rely on continuous data ingestion to refine models and optimise outputs. This is even more the case where AI agents are deployed across enterprise-level infrastructure. In practice, optimisation capacity is closely linked to the scale and diversity of data processed. In all cases, data collected for one operational purpose is often reused for analytics enhancement or behavioural calibration. This dynamic directly engages Article 5 (1)(b) (purpose limitation), Article 5 (1)(c) (data minimisation) and Article 6 (lawful basis) of the GDPR.

Under Article 6 (4), further processing must be assessed for compatibility with the original purpose. The CJEU has consistently emphasised strict adherence to purpose boundaries. In *Bara* (Case C-201/14), the CJEU held that repurposing personal data without proper notification and legal basis violates transparency principles. In *Breyer* (Case C-582/14), it confirmed that even dynamic IP addresses may constitute personal data where identification is reasonably possible.

Supervisory authorities are increasingly sceptical of broad reliance on legitimate interests under Article 6 (1)(f) for large-scale AI optimisation. Generic references to “service improvement” or “innovation” are arguably insufficient where processing materially affects individuals or involves behavioural profiling. Necessity and proportionality must be demonstrated concretely.

For non-European technology companies accustomed to expansive contractual data licences, this represents a structural compliance shift. European data protection law does not treat contractual permission as determinative of lawfulness. As confirmed in *Meta Platforms* (Case C-252/21), contractual framing cannot artificially broaden processing beyond what is objectively necessary.

Continuous optimisation models therefore sit in inherent tension with purpose limitation required under GDPR. Governance frameworks and product design must therefore anticipate this structural constraint.

Transparency, fairness and the substantive legitimacy of AI processing

As AI systems increasingly mediate access to services, information and economic opportunities, the legitimacy of processing turns not only on lawful basis and purpose limitation, but equally on transparency and fairness – two structural principles of EU data protection law. Transparency under Articles 13–15 GDPR and fairness under Article 5 (1)(a) are not ancillary disclosure obligations. They operationalise the fundamental right to data protection and structure the relationship between organisations and individuals whose data is processed.

In AI contexts, transparency operates as a precondition of legitimate deployment. Where individuals cannot meaningfully understand the nature, logic or implications of automated systems affecting them, the substantive lawfulness of processing becomes difficult to sustain. Legitimacy under the GDPR is not secured through formal compliance alone; it depends on whether processing remains aligned with reasonable expectations and fundamental rights protections.

The CJEU’s jurisprudence reinforces this orientation. In *Meta Platforms* (Case C-252/21), the court clarified that reliance on contractual necessity under Article 6 (1)(b) requires objective necessity, not strategic drafting. More broadly, the judgment confirms that fairness functions as a substantive constraint on how processing operations are structured and justified. It is not merely a formal recital-level principle.

These principles have concrete implications for AI systems that infer preferences, assign behavioural risk categories, personalise outputs or structure opportunities in ways that materially influence individuals. Generic disclosures or abstract descriptions of “AI use” may fail to satisfy transparency and fairness requirements. Supervisory authorities increasingly assess whether individuals receive intelligible explanations of the logic involved and the foreseeable consequences of profiling or automated evaluation.

Transparency obligations under Articles 13–15, GDPR require the provision of meaningful information about the logic involved, as well as the significance and envisaged consequences of processing. While

sometimes described as a “right to explanation”, this entitlement is legally framed as a right of access and transparency rather than full algorithmic disclosure. The obligation concerns intelligibility and practical comprehensibility – not the disclosure of source code or proprietary model architecture.

In algorithmic management systems, transparency cannot be reduced to a notice-layer exercise. Where automated or algorithmically influenced evaluations shape professional opportunities, remuneration, access or progression, explanations must enable individuals to understand the rationale and, where appropriate, to challenge it. Formal human oversight without informational clarity will not satisfy this standard.

The AI Act reflects this heightened sensitivity. Its transparency provisions – including obligations to inform individuals when interacting with certain AI systems and to disclose specific high-risk techniques such as emotion recognition or biometric categorisation – institutionalise a system-level expectation of intelligibility. However, these obligations supplement rather than displace the GDPR’s broader framework of transparency, fairness and proportionality. Where personal data is processed, legitimacy remains anchored in the GDPR.

Enterprise AI governance therefore requires dual attention: ex ante risk assessment through robust DPIAs under Article 35, and ongoing compliance with transparency, accountability and proportionality principles under Articles 5 and 13–15. In European regulatory practice, transparency is inseparable from legitimacy. It is measured not by the presence of formal disclosures, but by whether individuals can meaningfully understand how automated systems structure decisions, opportunities and outcomes affecting them.

Enterprise AI, algorithmic management and processor exposure

The regulatory exposure of enterprise AI systems does not arise solely at the point of automated decision-making. It emerges equally from the institutional embedding of algorithmic evaluation and AI use across an organisation.

In workforce and enterprise environments, AI systems and agents are not discrete customer-facing tools but embedded components of organisational governance and managerial oversight. They structure recruitment pipelines, allocate tasks, monitor productivity, score performance, prioritise procurement flows and model workforce optimisation. Their function is managerial rather than transactional.

Where personal data is processed in such environments, the GDPR analysis extends beyond Article 22 and automated decision-making (as discussed above). Articles 5 and 6, GDPR govern lawfulness, purpose limitation and proportionality. More structurally, Article 35, GDPR requires controllers to conduct a data protection impact assessment (DPIA) where processing is likely to result in a high risk to the rights and freedoms of natural persons.

Systematic and extensive evaluation of individuals based on automated processing – particularly where combined with large-scale monitoring – is expressly identified as a trigger for DPIA obligations. In workforce contexts, this threshold is frequently met. Continuous monitoring, predictive analytics and performance modelling operate within an environment of institutional power asymmetry, amplifying the potential impact on individuals’ rights.

However, the shift in enterprise AI governance lies not only in Article 22 exposure, but in the scale, persistence and organisational centrality of algorithmic use – especially as organisations migrate toward agent-based architectures. What was previously episodic assessment becomes continuous evaluation. What was once advisory becomes embedded into managerial infrastructure.

Supervisory authorities have demonstrated particular sensitivity to such deployments. DPIAs in this context must go beyond formal documentation. They require substantive assessment of necessity, proportionality, data minimisation and the effectiveness of safeguards – including meaningful human review mechanisms. Where residual high risk remains, Article 36 GDPR may require prior consultation with supervisory authorities before processing commences.

This governance shift also has material consequences for processors and technology suppliers. While the obligation to conduct a DPIA rests formally with the controller, the practical burden increasingly extends to processors and technology suppliers.

Article 28 (3)(f), GDPR requires processors to assist controllers in ensuring compliance with Articles 32–36, including DPIA preparation and prior consultation where required. In the context of enterprise AI systems, this assistance is no longer limited to generic security documentation. Our experience is that European customers increasingly expect detailed technical descriptions of model functionality and training logic; clear articulation of data inputs, outputs and processing flows; documentation of override mechanisms and human review pathways; risk mitigation descriptions aligned with DPIA frameworks; and transparency matrices mapping system features to GDPR safeguards.

This expectation is reinforced by the AI Act's documentation architecture, which requires high-risk system providers to maintain detailed technical files, risk management systems and data governance documentation. Even where the AI Act does not formally apply, enterprise customers increasingly replicate its structure contractually.

Accordingly, procurement practice has evolved. It is now common for European enterprise customers to require AI-specific contractual appendices sitting alongside data processing agreements. These AI appendices typically address: allocation of controller and processor roles in model deployment; use of customer data for model training or improvement; explainability and transparency commitments; audit rights relating to algorithmic governance; security measures and incident reporting specific to AI systems; and limitations on autonomous system modification or retraining. This development shifts AI governance into the contractual layer. Risk allocation becomes central. Providers must therefore carefully delineate the scope of their processing activities and the boundaries between customer-configured decision logic and system architecture alongside the extent of assistance obligations under Article 28 and the limits of liability relating to customer-defined deployment contexts.

Without careful structuring, providers risk de facto assumption of controller-level exposure through overly broad contractual commitments.

At the same time, resistance to reasonable assistance is commercially untenable. Enterprise customers – particularly in regulated sectors – increasingly require substantive DPIA support and structured co-operation in supervisory engagement. The provider response must therefore be calibrated: offering documented assistance, transparency and structured governance support, while maintaining clear contractual allocation of responsibility for lawfulness determinations and deployment choices.

For processors and suppliers, it additionally requires structured contractual governance, calibrated assistance under Article 28 and careful risk allocation in AI-specific appendices.

In this environment, compliance is no longer confined to the legality of discrete automated decisions. It extends to the architecture of organisational oversight – and to the contractual frameworks through which AI systems are supplied, configured and governed.

Data sovereignty, international transfers and essential equivalence

International data transfers remain one of the most structurally sensitive aspects of EU data protection law.

In *Schrems II* (Case C-311/18), the CJEU invalidated the EU–US Privacy Shield and clarified that transfer mechanisms under Article 46 must ensure “essentially equivalent” protection in practice. The Court emphasised substantive assessment of third-country legal regimes.

The subsequent adoption of the EU–US Data Privacy Framework (Commission Implementing Decision (EU) 2023/1795) under Article 45 has reintroduced a presumption of adequacy for participating US organisations and thus stabilised transatlantic transfers. However, adequacy does not eliminate accountability obligations under Articles 5 and 32.

Recent enforcement demonstrates the continued sensitivity of transfer risk. In 2025, the Irish Data Protection Commission imposed a EUR530 million fine on TikTok Technology Limited, finding that transfer impact assessments had not sufficiently addressed Chinese legal risks. The decision reinforces that documentation alone cannot compensate for deficiencies in substantive risk assessment or technical safeguards.

For AI systems operating across distributed infrastructure, transfer risk extends beyond hosting location. Remote administrative access, cross-border inference processing and sub-processor chains may constitute transfers under Article 44. In AI ecosystems characterised by continuous optimisation and federated infrastructure, data flows are often dynamic rather than static, complicating transfer mapping and impact assessments.

Beyond strict legal doctrine, data sovereignty has also evolved into both a regulatory and a commercial expectation. European enterprise customers increasingly request EU-based hosting, regional inference endpoints and contractual restrictions on secondary training uses. These requirements often exceed minimum legal standards, but reflect heightened sensitivity to strategic autonomy and geopolitical risk.

Accordingly, transfer compliance is no longer a discrete legal assessment but an architectural consideration. Data sovereignty increasingly shapes infrastructure design, vendor selection and governance strategy, reinforcing the GDPR's role as the constitutional benchmark for cross-border data flows.

Special categories and inference risk

Article 9, GDPR prohibits processing of special categories of personal data, subject to limited exceptions. These categories – including data revealing health, political opinions, religious beliefs, trade union membership, genetic and biometric data – reflect heightened constitutional sensitivity within the EU legal system.

AI systems capable of large-scale inference significantly complicate this framework. Supervisory authorities have indicated that outputs revealing health status, political opinions or ethnic origin may fall within

Article 9, even where not explicitly collected. In this respect, the legal qualification of processing may turn not only on the nature of the data collected, but on the attributes that can reasonably be derived from them.

The CJEU's protective jurisprudence in cases such as *OT v Vyriausioji tarnybinės etikos komisija* (Case C-184/20) supports broad interpretation of sensitive data protections. The court has consistently emphasised that Article 9 must be interpreted in light of its objective of ensuring enhanced protection for data that exposes individuals to particular risks of discrimination or social exclusion.

For AI systems deployed in biometric identification, behavioural analytics, sentiment analysis or predictive profiling contexts, inference capability becomes legally determinative. The assessment must consider both input data and the reasonably foreseeable outputs that a model is capable of generating. A system that derives sensitive attributes through probabilistic modelling may fall within Article 9 even if such attributes were not intentionally targeted.

The expansion of inference capability therefore broadens the potential scope of Article 9 beyond traditional data collection paradigms. In AI-driven environments, sensitive data risk arises not only from what is collected, but from what can be inferred.

Conclusion: procedural recalibration and strategic positioning in 2026

Taken together, the AI Act, the Data Act, the DMA, the DSA and related cybersecurity instruments represent not fragmentation but consolidation within the Union's digital framework. However, none of these instruments displace the GDPR's constitutional status. Where personal data is processed, the assessment of digital systems continues to be anchored in the GDPR's principles of lawfulness, purpose limitation, fairness, transparency and accountability.

For technology providers, this architecture precludes siloed compliance. AI Act risk classification, data governance obligations under the Data Act, platform responsibilities under the DSA and competition-facing duties under the DMA intersect with, rather than replace, data protection governance. Risk assess-

ment, impact analysis, automated decision-making safeguards and transfer architecture must therefore be evaluated within a unified compliance framework grounded in the GDPR's substantive requirements.

This convergence of regulatory regimes – spanning data protection, competition, consumer protection and strategic autonomy – elevates digital governance to a matter of enterprise-wide risk management rather than discrete legal compliance. It increasingly demands oversight at the highest organisational levels.

Within this consolidated architecture, the Digital Omnibus signals procedural recalibration rather than substantive retreat. It seeks to streamline supervisory co-ordination without altering the underlying constitutional logic. Supervisory authorities remain guided by CJEU jurisprudence that consistently interprets data protection as a fundamental right requiring effective and practical protection.

For non-European technology companies, the strategic insight is therefore not merely that regulation is increasing in volume. Rather, the enforcement logic of the Union's digital framework has stabilised around constitutional principles – fairness, proportionality, accountability and sovereignty – which now permeate the expanding rulebook.

The European Union is not downgrading its regulatory model; it is consolidating and systematising it. In this environment, embedding privacy, risk governance and architectural accountability at the design stage is not a defensive compliance strategy but a structural condition for sustainable participation in the European market.

FRANCE



Law and Practice

Contributed by:

Sylvain Naillat and Helena Delabarre
Nomos

Contents

1. Legal and Regulatory Framework p.113

- 1.1 Overview of Data and Privacy-Related Laws p.113
- 1.2 Rights and Obligations p.114
- 1.3 Special Categories of Personal Data p.115
- 1.4 Processing of Personal Data for Research and Development Purposes p.115
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.116
- 1.6 Data Breach Requirement p.117
- 1.7 Regulators p.118
- 1.8 Enforcement Proceedings and Fines p.119
- 1.9 Enforcement Trends p.120

2. Privacy Litigation p.120

- 2.1 Privacy Litigation Overview p.120
- 2.2 Recent Case Law p.121
- 2.3 Collective Redress Mechanisms p.122

3. Requirements for the Protection and Processing of Non-Personal Data p.122

- 3.1 Objectives and Scope of Data Regulation p.122
- 3.2 Interaction of Data Regulation and Data Protection p.122
- 3.3 Rights and Obligations Under Applicable Data Regulation p.123
- 3.4 Regulators and Enforcement p.123

4. Sectoral Topics p.124

- 4.1 Use of Cookies p.124
- 4.2 Personalised Advertising and Other Online Marketing Practices p.124
- 4.3 Employment Privacy Law p.125
- 4.4 Data Protection in M&A p.125

5. International Considerations p.126

- 5.1 Restrictions on International Data Transfers p.126
- 5.2 Government Notifications and Approvals p.126
- 5.3 Data Localisation Requirements p.126
- 5.4 Blocking Statutes p.127
- 5.5 Recent Developments p.127

Nomos is an independent business law firm bringing together approximately 40 lawyers and legal professionals. The firm advises and represents clients in both advisory and litigation matters, in France and internationally. In an evolving legal and regulatory environment, Nomos combines precision, strategic vision and responsiveness. Its practice is grounded in a detailed understanding of sector-specific economic and financial challenges, enabling the firm to support innovative and complex business models. It has particular strength in technology, data protection, IP, entertainment and regulated sectors, positioning the

firm at the forefront of digital and market transformations. Nomos adopts a comprehensive, 360-degree approach, integrating sharp sector knowledge, legal creativity and a results-oriented mindset. Its teams are committed, agile and focused on building trust-based, long-term relationships. The firm's main areas of practice include technology and data protection; media and entertainment; IP; competition and consumer law; corporate/M&A; tax; employment; health-care and life sciences; business litigation; and non-profit and professional organisations law.

Authors



Sylvain Naillat is a partner in Nomos' IP-tech-media team. He advises French and international clients on data protection and technology matters, including structuring, drafting and negotiating commercial and

technology contracts, and assessing new products and services, particularly within complex digital ecosystems such as online advertising. He assists organisations in designing and implementing privacy governance and compliance programmes. Sylvain regularly represents clients in high-stakes litigation and investigations before the French courts and the CNIL. He also advises and litigates in media law and literary and artistic property, especially in the music and audio-visual sectors. He is admitted to the Paris and California bars.



Helena Delabarre has been co-leading Nomos' IP-tech-media team since 2002. She focuses on data privacy, intellectual property and information technology, where she advises e-commerce leaders,

consumer electronics manufacturers and media group companies. In the field of data privacy, she has notably strong experience in the defence of international clients against the CNIL's enforcement actions.

Nomos

49 avenue de l'Opéra
75002 Paris
France

Tel: +33 (0)1 43 18 55 00
Email: contact@nomosparis.com
Web: www.nomosparis.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

General Legal Framework

France's data protection and privacy landscape is built upon a two-tier regulatory structure combining European Union law with national legislation. The cornerstone of this framework is the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which has been directly applicable since 25 May 2018, and serves as the primary legal instrument establishing minimum standards for data protection across all EU member states, including France. Under French domestic law, the main regulatory instrument for the protection of personal data is the French Data Protection Act (FDPA) – known as “*Loi informatique et libertés*”, which was originally enacted on 6 January 1978 (Law No 78-17) and has been amended several times since.

The interaction between the EU texts and the FDPA is hierarchical but complementary: the GDPR sets the harmonised standard, while the FDPA:

- fills gaps left by the GDPR – for example, the FDPA contains rules on the fate of personal data after the death of the data subjects, which are expressly excluded from the GDPR's scope;
- introduces specific requirements and protection pursuant to the GDPR's opening clauses – for example, the FDPA defines a specific regulatory framework to process health data in the context of research projects;
- transposes the EU Law Enforcement Directive (2016/680), as well as the cookie provisions of the EU ePrivacy Directive (2002/58), into French Law; and
- delineates the powers of the national regulator, the National Commission for Information Technology and Civil Liberties (*Commission Nationale de l'Informatique et des Libertés* – CNIL).

Sectoral Legal Instrument

Sectoral instruments also play an important role. The Public Health Code (*Code de la santé publique*) contains particular provisions governing the processing of health data, including requirements for hosting certi-

fication (“HDS certification”). The Post and Electronic Communications Code (*Code des postes et des communications électroniques* – CPCE) governs electronic marketing and the confidentiality of correspondence, transposing the ePrivacy Directive. Furthermore, the Labour Code (*Code du travail*) regulates employee monitoring, requiring proportionality and prior consultation with employee representative bodies.

Extraterritorial Reach

Both the GDPR and the FDPA have significant extraterritorial reach. Under GDPR Article 3, the regulation applies to organisations established in the EU, regardless of where data processing occurs; and to organisations established outside the EU that offer goods or services to data subjects in the EU or monitor their behaviour. This territorial principle is reproduced in the FDPA. Regarding specifically the “opening provisions”, the FDPA states that French rules apply as long as the data subject resides in France, including when the data controller is not established in France.

Interplay with Non-Personal Data, Cybersecurity, and AI Regulation

France's regulatory framework increasingly integrates data protection with rules on non-personal data, cybersecurity and AI.

- The Data Act (Regulation (EU) 2024/1864), applicable from September 2025, governs data access and sharing – especially for IoT data – and overlaps with the GDPR where personal data is involved; France's 2024 SREN Law (*Loi sur la Sécurité et Régulation des Espaces Numériques*) complements this by imposing interoperability and portability duties on cloud providers.
- The French cybersecurity agency, ANSSI (*Agence nationale de la sécurité des systèmes d'information*) enforces NIS and NIS2 obligations, requiring incident notifications that may also trigger GDPR breach reporting to the CNIL.
- The AI Act (Regulation (EU) 2024/1689), phased in until August 2027, applies cumulatively with the GDPR when AI systems process personal data, requiring organisations to comply simultaneously with both AI-specific and data protection requirements.

1.2 Rights and Obligations

General Principles for Personal Data Processing

The processing of personal data in France is governed by foundational principles established in the GDPR and reflected in the FDPA. These principles constitute the normative framework within which all data processing must occur.

- **Lawfulness, fairness and transparency:** All processing must be lawful, fair, and transparent. Lawfulness requires a valid legal basis under GDPR Article 6 (or FDPA Article L 13-13), which includes consent, contract performance, legal obligation, vital interests, public task, or legitimate interests. Fairness requires that processing must be carried out honestly and without deception. Transparency mandates providing clear information to data subjects regarding the main aspects of processing.
- **Purpose limitation:** Personal data may be processed only for specified, explicit and legitimate purposes. Any use beyond the original purpose requires a compatibility assessment or a new legal basis.
- **Data minimisation:** Only personal data that is adequate, relevant, and strictly necessary for the specified purposes may be collected and processed.
- **Accuracy:** Personal data must be accurate and kept up to date, with reasonable measures taken to rectify or delete inaccurate data.
- **Storage limitation:** Personal data must be kept only as long as necessary for the processing purpose.
- **Security:** Personal data must be processed securely and protected against unauthorised access, alteration, loss or destruction through appropriate technical and organisational measures.
- **Accountability:** Data controllers must demonstrate compliance with all principles through documentation, records, impact assessments, and governance structures.

Data Subject Rights

The GDPR grants individuals a broad set of enforceable rights over their personal data. These include the right to access and obtain information about how their data is processed, to rectify inaccurate data, and, where legally justified, to request erasure. Data subjects may also restrict processing, receive their data in

a portable and machine-readable format, and object to certain types of processing, including marketing or processing based on legitimate interests or public tasks. In addition, they are protected against purely automated decision-making, with the right to seek explanations and human review, and they may lodge complaints with a supervisory authority free of charge.

The FDPA adds a specific data subject right, linked to digital death: Article 85 of the FDPA allows individuals to define general or specific directives concerning the storage, erasure and communication of their personal data after their death.

Organisational Compliance: Essential Checklist

- **Apply privacy by design/default:** Embed data protection principles from the design phase of products or services.
- **Establish a legal basis:** Identify and document a valid legal basis (GDPR Article 6) for each processing purpose and reassess when purposes or conditions change.
- **Define retention and deletion rules:** Establish structured retention periods and ensure systematic, preferably automated deletion backed by documented reviews.
- **Ensure adequate security measures:** Implement technical and organisational safeguards appropriate to processing risks, including encryption, access controls, testing, and incident response plans.
- **Provide transparent information:** Supply complete privacy information at collection (at first contact or within one month when collection is indirect), covering all mandatory items listed under Article 13 (direct collection) or 14 (indirect collection) of the GDPR.
- **Enable data subject rights:** Set up practical processes to exercise rights easily, ensuring effective access, objection, deletion, restriction, etc.
- **Manage third-party processing:** Contractually define data protection obligations when working with external processors or controllers.
- **Conduct data protection impact assessments (DPIAs):** For high-risk processing, perform DPIAs outlining risks and mitigation measures.
- **Appoint a data protection officer (DPO):** Organisations that do extensive or sensitive data process-

ing must designate an independent, qualified DPO who reports directly to senior management.

- Document compliance.

1.3 Special Categories of Personal Data Prohibition on Processing Special Categories of Personal Data

Under Article 9 GDPR, processing of special categories of personal data (including data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, and genetic, biometric, or health data) is prohibited unless a specific derogation applies.

Derogations include, among other things:

- obtaining the explicit consent of the data subject to the processing of such data;
- specific obligations and rights in the fields of employment, social security, or social protection law;
- protection of the vital interests of the data subject when they are physically or legally incapable of giving consent;
- preventative or occupational medicine, medical diagnosis, and the management of health or social care systems and services – generally under the responsibility of a professional subject to confidentiality obligations;
- public interest in the field of public health, eg, monitoring epidemics; and
- archiving in the public interest, for scientific or historical research purposes, or statistical purposes, subject to appropriate safeguards.

Specific hosting requirement for health data

Where health data is hosted for care-related activities, French law requires use of a certified host (“Health Data Hosting Provider” – Article L 1111-8 of the Public Health Code), with contractual constraints.

Processing data related to criminal convictions

Personal data related to criminal convictions is not among the special categories where processing is prohibited by principle under Article 9 of the GDPR. However, it is also subject to specific rules. Under Article 46 of the FDPA (implementing Article 10 GDPR), processing data regarding criminal convictions is largely a

state monopoly, reserved for courts and public authorities. Private entities are strictly limited in their ability to process such data. Employers, for example, cannot conduct blanket criminal background checks; they may only request a criminal record extract (Bulletin No 3) if it is strictly necessary for the job and authorised by law (eg, for security personnel or employees working with minors).

Protecting minors’ data

Following the GDPR, the age of digital consent for the processing of personal data in France is 15, meaning that children under 15 cannot validly consent to the processing of their data by online services without parental authorisation. Organisations must implement proportionate age verification or parental consent mechanisms and ensure that data collection remains strictly necessary. More broadly, the protection of minors is a crucial and highly topical issue in France. At the time of writing, parliamentary debates are underway regarding a proposed ban on social media for those under the age of 15.

1.4 Processing of Personal Data for Research and Development Purposes Scientific Research (Including Health Research, Studies and Evaluations)

The GDPR recognises a research-oriented regime: further processing for scientific research is, subject to Article 89 safeguards, not considered incompatible with the initial purpose (Article 5 (1)(b)), and member state law may allow limited derogations from certain data-subject rights where necessary and proportionate.

To process health data (see 1.3 Special Categories of Personal Data), controllers commonly rely on the scientific research ground (Article 9 (2)(j)) coupled with Article 89 safeguards.

France adds a specific gatekeeping layer for health-sector “research/study/evaluation” processing: such processing must pursue a public-interest purpose and either comply with a CNIL reference methodology (in which case, it can proceed after filing a simple declaration of compliance) or have obtained specific authorisation from the CNIL.

The CNIL reference methodologies include MR-001 (scientific research requiring patients' consent), MR-003 (certain research without patient's consent but with information and a right to object) and MR-004 (secondary-use studies/research not involving the person).

Product and Service Development

If R&D is primarily product improvement, commercial analytics or model training, it may not qualify as "scientific research" and should be assessed under ordinary GDPR rules: a valid Article 6 legal basis plus, if health data or other special categories of data are processed, an Article 9 (2) condition (often explicit consent). Re-use of consent-based data beyond the original scope generally requires new consent or a new legal basis.

Anonymisation as a Data Protection Safeguard

The legal provisions outlined above governing scientific research and product or service development apply to the processing of "personal" data. Where such data is anonymised in accordance with principles and technical requirements, ensuring no reasonable risk of re-identification (notable in accordance with WP29 Opinion 05/2014), it ceases to constitute personal data. As a result, it falls outside the scope of the GDPR and may be used freely for research or development purposes.

True anonymisation is therefore a key privacy protection mechanism and is encouraged in all cases. Moreover, when identifiable data is not strictly necessary for the intended processing, anonymisation is required to comply with the GDPR's data minimisation principle.

Anonymisation must not be confused with pseudonymisation. Pseudonymisation replaces direct identifiers (eg, name, surname) with a code (eg, a number), but the data remains personal as long as a re-identification key exists. A recent CJEU ruling held that, in certain situations, pseudonymised data may be considered anonymous for a third party that cannot reasonably access the key or other re-identifying information.

The European Health Data Space (EHDS)

Regulation (EU) 2025/327 establishing the European Health Data Space (EHDS), will create a harmonised EU framework for accessing and re-using electronic health data. It will apply from 26 March 2027, with the core secondary-use regime becoming operational on 26 March 2029. For life sciences companies, the EHDS establishes a structured EU-wide pathway for secondary use of electronic health data through data permits issued by national Health Data Access Bodies (HDABs) or health data requests, including for scientific research and related development or innovation activities (such as algorithm training and evaluation).

Access must occur exclusively within a secure processing environment with strict technical and organisational controls, including restricted access and mandatory audit logs. Only non-personal, anonymised outputs may be exported. Certain purposes – such as advertising or marketing – and any form of re-identification are expressly prohibited. Results of secondary use must be published in anonymised form within 18 months. Individuals may opt out of secondary use of their personal electronic health data; where identifiable, their data may not be used for new permits or newly approved requests, subject to limited exceptions under national law.

Enforcement risks are significant: fines may reach EUR10 million or 2% of global turnover, going up to EUR20 million or 4% of global turnover for serious infringements (including prohibited uses, extraction of personal data from secure environments, and re-identification). The EHDS applies alongside the GDPR, meaning that parallel GDPR liability may arise.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Applicability of Data Protection Laws to AI

In France, the personal data regulatory framework, comprising the EU GDPR and the FDPA, fully applies to the processing of personal data through AI systems. The GDPR already includes rules that are particularly relevant for AI systems, such as the prohibition – subject to certain exceptions – of fully automated decisions that produce legal effects or significantly affect the individuals concerned (Article 22 of the GDPR).

CNIL's AI Guidance

The CNIL has positioned itself as a key AI regulator by issuing guidance in 2024–2025 on how the GDPR applies to AI systems. Its recommendations address core issues such as choosing a lawful basis, complying with data minimisation and transparency principles, conducting DPIAs, managing data subject rights, securing AI development, mitigating bias, and ensuring proper documentation and accountability, thereby promoting a risk-based and integrated compliance approach.

Overlay of the EU AI Act

The AI Act (Regulation (EU) 2024/1689) establishes a risk-based compliance framework distinct from, but complementary to, EU data protection law. It introduces prohibitions, transparency duties, and extensive obligations for high-risk AI systems and certain general-purpose models. Application is being phased in between 2025 and 2027 (prohibitions from February 2025; general-purpose model obligations from August 2025). It does not affect the GDPR (Article 2 (7)).

- **Transparency:** Providers of high-risk systems must prepare technical documentation (Article 11) and clear instructions for use enabling risk assessment and mitigation (Article 13), including, where relevant, a DPIA (Article 26 (9)). Specific information duties apply towards individuals, eg, disclosure of AI interaction or synthetic/deepfake content (Articles 50, 26 (11)).
- **Data governance:** High-risk system providers must implement documented governance for training, validation, and testing data, ensuring relevance, representativeness, quality, traceability, and bias mitigation. Limited processing of special categories of data is permitted strictly for bias monitoring under enhanced safeguards (Article 10).
- **Human oversight:** High-risk systems must enable effective human control (interpretation, override, interruption, disregard of outputs) (Article 14). Deployers must assign oversight to competent persons with appropriate authority (Article 26 (2)), reinforcing fundamental-rights safeguards, including data protection.

1.6 Data Breach Requirement

Under Article 33 of the GDPR, data controllers must notify the competent data protection authority of any personal data breach not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. In France, this notification is typically done via CNIL's dedicated online portal. Furthermore, if the breach is likely to result in a high risk to the rights and freedoms of a natural person, Article 34 of the GDPR imposes controllers to communicate the personal data breach to the data subject "without undue delay".

Cross-Reporting

In France, the notification landscape in case of a security incident is fragmented. For example, where an entity is subject to the NIS framework, it must separately notify ANSSI of significant cyber-incidents. For financial entities, the EU Digital Operational Resilience Act (DORA) requires the notification of major ICT-related incidents to the "competent authority". In France, depending on the type of financial entity concerned, this will generally be the *Autorité de contrôle prudentiel et de résolution* (ACPR) and/or the *Autorité des marchés financiers* (AMF). At the time of writing, the European Commission has proposed, as part of a digital regulatory simplification initiative (often referred to as the "Digital Omnibus"), the creation of a single reporting entry point intended to streamline notifications under several EU digital frameworks (including NIS2, the GDPR and DORA). This remains a legislative proposal and is not yet in force.

Action Items for Organisations

- **Immediate assessment:** Upon detection, the organisation must assess the nature of the breach, the categories of data (eg, sensitive v non-sensitive), the volume of data subjects affected, and the likely consequences. The goal is to assess the level of risk for data subjects (and thus what notification obligations apply) and determine the remediation measures that must be implemented to contain the incident and avoid its repetition.
- **Notify the CNIL (unless risks for data subjects are unlikely):** Submit breach notification to the CNIL within 72 hours via the online portal, with sufficient specificity.

- Notification to data subjects: If the breach poses a “high risk” to individuals (eg, risk of identity theft, fraud or discrimination), the controller must communicate the breach to the data subjects without undue delay, providing clear advice on how to protect themselves (Article 34 GDPR).
- Additional actions: Controllers will often also consider filing a criminal complaint and notifying their cyber-insurance provider (typically also within 72 hours).
- Documentation: All breaches, including those not notified to the CNIL, must be recorded in an internal breach register, detailing the facts, effects and remedial actions taken. This register is often one of the first documents requested during a CNIL inspection.

Recent enforcement actions, such as the EUR5 million fine against France Travail in 2024 and the EUR45 million fine against the internet access provider FREE in 2025 following massive data leaks, underscore the CNIL’s intolerance for failures in basic security hygiene and breach response.

1.7 Regulators

France employs a multi-regulator model for the digital space, requiring organisations to navigate overlapping jurisdictions.

French Data Protection Authority

The CNIL acts as the French guardian of data privacy. Its missions and powers include:

- Standards and guidelines – it develops frameworks for sectors like AI, health data, and cookies. While technically “advisory”, these are treated as authoritative by the courts.
- Public awareness – it provides educational resources and tools (templates, checklists) for the public and small businesses.
- Investigative procedures – investigations are triggered either by individual complaints (approximately 4,000/year) or self-initiated audits by the CNIL.
- Enforcement powers – the CNIL has broad legal authority to ensure compliance, including by issuing administrative fines (up to EUR20 million or 4% of the worldwide annual turnover, whichever is

higher), public reprimands or injunctions, or revoking certifications.

The CNIL operates within a network of regulators:

- Domestic – it notably co-ordinates with ANSSI (cybersecurity), the ACPR (finance), and the ARCEP (telecoms).
- International – as a member of the European Data Protection Board (EDPB), it works with other EU authorities to ensure consistent application of the GDPR across borders.

Sectoral Authorities

- ANSSI (the National Cybersecurity Agency of France) is the authority dealing with cyber-defence and resilience. It enforces the NIS Directive and certifies security products (eg, SecNumCloud). ANSSI focuses on technical standards and critical infrastructure protection.
- ARCEP (*Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse*) has been empowered by the SREN Law and the Data Governance Act to regulate data intermediation services and the cloud computing market (specifically regarding switching and interoperability).
- ARCOM (*Autorité de régulation de la communication audiovisuelle et numérique*) acts as the digital services co-ordinator for France under the Digital Services Act (DSA) and oversees certain aspects of platform regulation, particularly regarding the protection of minors online.
- The DGCCRF (*Direction générale de la concurrence, de la consommation et de la répression des fraudes*) is the Directorate General for Competition, Consumer Affairs and Fraud Control, which focuses on consumer protection aspects of digital platforms, including dark patterns and transparency in online marketplaces.
- The ACPR (*Autorité de contrôle prudentiel et de résolution*) is the French Prudential Supervision and Resolution Authority, which supervises financial institutions and addresses data protection and cybersecurity standards alongside financial regulation.
- The ANSM (*L’Agence nationale de sécurité du médicament et des produits de santé*) is the

National Agency for the Safety of Medicines and Health Products. It oversees medical device manufacturers' data protection compliance, particularly concerning patient data processing and device security.

These authorities notably co-ordinate through a formal national network established by the SREN Law to ensure consistent application of the DSA.

1.8 Enforcement Proceedings and Fines Investigation Initiation and Procedures

The CNIL generally initiates investigations based on complaints, external reports, data breach notifications, or on its own initiative when it identifies a sensitive risk area or sector. It may investigate any controller or processor through unannounced on-site inspections, document-based reviews, hearings, or online checks of websites and services.

During these investigations, the CNIL collects documents, interviews staff and examines systems to assess compliance with the GDPR and the FDPA. An investigation can close with no further action, or the CNIL's president may issue a formal notice (*mise en demeure*) giving the organisation a deadline within which to comply. This notice is not a sanction but a warning phase. If breaches are serious, persistent or unresolved, the president may – whether or not a prior notice was issued – refer the case to the CNIL's sanctions committee (*formation restreinte*), which is responsible for imposing sanctions.

Once referred, a formal sanctions procedure begins: the president appoints a rapporteur, who exchanges written submissions with the organisation and may hold a hearing. The case is then transmitted to the sanctions committee for an adversarial decision. The CNIL has no power to settle cases.

Sanctions imposed by the panel are immediately enforceable, and fines are paid to the French Treasury (meaning they do not finance the CNIL). Decisions can be appealed before the Conseil d'État.

For less serious cases, a simplified procedure allows the president of the sanctions committee or a designated member to decide alone, without a public hear-

ing, with lower maximum fines (up to EUR20,000) and limited publicity – enabling the CNIL to handle a higher volume of straightforward infringements.

Available Sanctions and Remedies

Administrative sanctions

- Warnings: Formal notice of non-compliance without financial penalties, typically for minor violations or first-time offences where organisations demonstrate rapid remediation.
- Injunctions to cease processing: Orders requiring organisations to halt specific data processing within defined timeframes.
- Interim injunctions with daily penalties: Injunctions compelling specific corrective actions (to implement data protection policies, delete unlawful data or implement security measures) with daily penalty assessments (up to EUR100,000 per day) for non-compliance.
- Administrative fines: Monetary penalties up to EUR20 million or 4% of the annual worldwide turnover (whichever is higher) pursuant to GDPR Article 83.
- Certification revocation: Where organisations hold CNIL certifications, the CNIL may revoke these, effectively prohibiting certification-dependent activities.
- Public disclosure: CNIL decisions, particularly those imposing significant fines, are typically published (sometimes, but seldom, in anonymised form).

Civil remedies

Beyond CNIL administrative sanctions, data subjects may pursue civil damages before the French judicial courts (pursuant to GDPR Article 82).

Criminal sanctions

Serious data protection violations may trigger criminal sanctions under the French Criminal Code, which criminalises, among other things:

- failure to implement security measures (Article 226-17);
- the processing of special categories of personal data without legal basis (Article 226-19); or
- failure to notify personal data violations (Article 226-17-1).

Criminal penalties include fines up to EUR300,000; imprisonment for up to five years; and publication of conviction decisions. However, criminal prosecution is very rare in practice. The CNIL refers cases to prosecuting authorities where criminal elements appear evident, but prosecutors exercise prosecutorial discretion in pursuing charges.

Aspects Used to Set Penalty Levels

The CNIL applies the criteria set out in Article 83 (2) of the GDPR to determine the amount of the fine, including the seriousness and impact of the infringement, whether the conduct was intentional or negligent, and the controller's efforts to mitigate damage. It also considers elements such as prior violations, the degree of co-operation with the authority, and the sensitivity of the personal data concerned.

It is important to note that the CNIL does not provide details on how it reaches a specific amount, including when that amount covers infringements of different natures. The absence of any obligation in this respect was confirmed by the French Supreme Administrative Court (Conseil d'État).

1.9 Enforcement Trends

Over the last approximately 24 months, data-protection enforcement in France has become both higher volume and higher impact. In 2024, the national regulator reported 331 corrective measures, including 87 financial penalties totalling EUR55,212,400, alongside a record 17,772 complaints. It also received 5,629 personal-data breach notifications (20% more than in 2023) and highlighted a rise in very large-scale incidents, noting that breaches affecting more than one million individuals doubled. In 2025, it issued 83 sanctions with cumulative fines of EUR486,839,500 and identified three recurring enforcement themes: cookies/trackers, employee monitoring, and data security.

Most significant enforcement trends:

- Cookies and trackers are driving the biggest exposure: there have been repeat findings to do with placing trackers without valid prior consent or providing sufficient user information, as well as failure to respect refusals or withdrawals of consent.

- Workplace surveillance under sustained scrutiny: enforcement emphasised that continuous or disproportionate employee monitoring, notably through video surveillance, is unlawful in the absence of exceptional, well-justified circumstances.
- Processor compliance in the spotlight: sanctions also addressed breaches of processors' obligations, recalling in particular the need to –
 - (a) implement appropriate technical and organisational security measures;
 - (b) process data only on the controller's documented instructions; and
 - (c) delete data at the end of the contractual relationship.
- Security of processing as a major enforcement driver: the regulator issued particularly heavy sanctions in 2025 for shortcomings in the security of processing, repeatedly underscoring the need to apply strict "baseline hygiene" measures (eg, strong authentication and access control, timely patching, secure configuration, least privilege, and monitoring).
- More frequent enforcement via streamlined procedures: the regulator attributes a sharp rise in the number of sanction decisions to its simplified process, increasing the likelihood of action against a broader set of organisations.

2. Privacy Litigation

2.1 Privacy Litigation Overview

General Trends

Over the last 24 months, personal data disputes in France have increasingly reached the courts through private enforcement of the GDPR. Two recurring streams stand out: (i) compensation claims following security incidents or unauthorised disclosures; and (ii) litigation seeking compliance with data-subject rights – particularly access requests, including in an employment context (eg, access to professional emails, subject to the rights of others).

Claimants are mainly individuals (customers, users, employees or former employees). Typical remedies include compliance orders (eg, to grant access, erase

data, or cease unlawful processing), sometimes subject to penalty payments, as well as damages.

Non-Material Damage

Non-material damage is compensable under Article 82 GDPR, but a mere infringement is insufficient. The claimant must prove:

- an infringement;
- actual damage (including non-material); and
- a causal link (*CJEU, C-300/21, Österreichische Post*).

No minimum seriousness threshold applies, yet harm must be real and proven.

Negative emotions (fear, anxiety, loss of control, reputational concern, risk of misuse) may qualify if substantiated and causally linked (*CJEU, C-340/21, Nat-sionalna agentsia za prihodite CJEU, C-655/23, Quirin Privatbank*). Purely hypothetical risk or unproven fear is insufficient.

Compensation is strictly compensatory, not punitive. It must reflect the actual damage suffered; fault is irrelevant to quantification once liability is established (*CJEU, C-667/21, Krankenversicherung Nordrhein*). A separate injunction under national law cannot reduce damages (*CJEU, C-655/23, Quirin Privatbank*).

The GDPR does not harmonise methods of calculation. Quantification remains subject to national procedural autonomy, constrained by equivalence and effectiveness, and Article 83 fine criteria cannot be transposed to Article 82 (*CJEU, C-741/21, juris GmbH*).

2.2 Recent Case Law

The court decisions that have most significantly shaped the framework for privacy litigation before the courts (ie, to be distinguished from the CNIL's GDPR enforcement cases through administrative proceedings) in recent years are described below.

Article 82 GDPR – Conditions and Nature of Compensation

- *CJEU, C-300/21, Österreichische Post* (4 May 2023): The court held that compensation requires proof of an infringement, actual damage, and a

causal link, and that a mere GDPR breach does not automatically entitle a claimant to damages. Non-material damage need not reach a seriousness threshold, but it must be proven, and compensation must remain purely compensatory under national rules subject to equivalence and effectiveness.

- *CJEU, C-741/21, juris* (11 April 2024): The court clarified that infringement of a GDPR right does not in itself constitute non-material damage, although “loss of control” may qualify if genuinely suffered. It further held that the fine criteria in Article 83 are irrelevant when assessing damages under Article 82.
- *CJEU, C-590/22, PS* (20 June 2024): The court recognised that proven fear of disclosure, together with its negative consequences, may constitute non-material damage, while reaffirming that Article 82 has no punitive or deterrent function.
- *CJEU, C-200/23, Agentsia po vpisvaniyata* (4 October 2024): The court held that temporary public accessibility of personal data may generate compensable “loss of control” even without additional tangible harm, provided actual damage is established.
- *CJEU, C-655/23, Quirin Privatbank* (4 September 2025): The court confirmed that negative emotions may amount to non-material damage if proven and causally linked, and it clarified that preventative injunctions cannot replace or reduce compensation under Article 82.

Structure of Liability and Exoneration

- *CJEU, C-667/21, Krankenversicherung Nordrhein* (21 December 2023): The court characterised Article 82 as establishing fault-based liability with a strict exoneration standard, under which the controller avoids liability only by proving that it is not in any way responsible for the event causing the damage.
- *CJEU, C-741/21, juris* (11 April 2024): The court confirmed that a controller cannot evade liability by attributing the infringement to a person acting under its authority.

GDPR Breach and Unfair Competition

CJEU, C-21/23, Lindenapotheke (4 October 2024): The court ruled that Chapter VIII of the GDPR does

not preclude national law from allowing competitors of an undertaking infringing the GDPR to bring civil proceedings against the undertaking for unfair commercial practices, where such infringement confers a competitive advantage on that undertaking.

2.3 Collective Redress Mechanisms Representation Under the GDPR

GDPR Article 80 allows individuals to mandate non-profit bodies, organisations or associations to lodge complaints and bring judicial proceedings on their behalf. Member states may also allow certain bodies to act without a mandate.

“Action de Groupe” and the 2025 Reform

France has allowed class-action style procedures (*action de groupe*) in specific sectors, including consumer matters and data protection. In 2025, France adopted a significant reform aimed at streamlining and expanding group actions (Law No 2025-391 of 30 April 2025). The new framework establishes a unified regime applicable across matters and is designed to facilitate claims for both cessation of unlawful conduct and compensation, subject to French procedural safeguards and typically an opt-in mechanism for claimants.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation The EU Data Act

The European Data Act (Regulation (EU) 2023/2854), adopted on 13 December 2023, entered into force on 11 January 2024 and has been applicable since 12 September 2025. It sets EU-wide rules on fair access to and use of data. It focuses on data generated by connected products and related services, and on switching and interoperability for data processing services (including cloud and edge computing services).

The regulation applies to situations involving both personal and non-personal data. Where personal data is concerned, the GDPR prevails in cases of conflict, and the Data Act operates without prejudice to EU data-protection law.

Scope and key mechanisms

- Product data and related service data: users of connected products are granted access rights to data generated by their use of the product or related service, including necessary metadata.
- B2B data sharing: data holders must make data available to third parties at the user’s request, subject to safeguards (eg, trade secrets).
- Public-sector access: public bodies may request data in cases of “exceptional need” under strict conditions.
- Cloud switching and portability: providers of data processing services must remove unjustified switching barriers and enable portability of customers’ exportable data and digital assets.

The regulation defines key roles, including users, data holders, data recipients, and, for cloud services, customers and providers of data processing services. It also references data intermediation services as defined in the Data Governance Act.

French Context

While the Data Act is EU-wide regulation, France has anticipated it with the “SREN” Law No 2024-449 of 21 May 2024 (Law to Secure and Regulate the Digital Space). The SREN Law establishes interoperability and portability obligations for cloud computing service providers, complementing Data Act requirements. This law addresses specific French concerns regarding data sovereignty and technological resilience.

3.2 Interaction of Data Regulation and Data Protection

A core principle of the EU Data Act is that, whenever personal data is involved, the GDPR continues to apply, and prevails in case of conflict. For mixed datasets (containing personal and non-personal data), the GDPR applies to the personal-data component. Where the two are technically or functionally inseparable, GDPR obligations cannot be bypassed and, in practice, the dataset must be handled under GDPR-compliant safeguards.

This interaction creates specific legal constraints. For example:

- Legal basis – The Data Act grants rights of access and sharing but does not create a standalone GDPR legal basis for processing personal data. Where disclosure involves personal data – especially if the requesting user is not the data subject – a valid GDPR legal basis must independently exist.
- Trade secrets and IP – The Data Act protects trade secrets and intellectual property. As a rule, access should be enabled with appropriate confidentiality measures; refusal to share on trade secret grounds is limited to narrowly defined and exceptional circumstances and cannot serve as a pretext to block legitimate access.

3.3 Rights and Obligations Under Applicable Data Regulation

Access and Sharing of Connected Product Data

The Data Act gives users of connected products and related services the right to access and share certain “readily available” product and related service data, including necessary metadata (Articles 3–7).

Accordingly, data holders must notably:

- design products for data accessibility (for products placed on the market from 12 September 2026);
- provide access without undue delay, free of charge, in a structured, commonly used, machine-readable format (including continuous/real-time access where relevant and technically feasible);
- enable user-directed sharing with third parties under equivalent conditions;
- respect the GDPR where personal data is involved;
- apply trade secret protections only where justified, proportionate and safeguarded; and
- ensure third-party use complies with statutory limitations.

B2B Fairness and Cloud Switching

The Data Act controls unfair terms in B2B data-sharing contracts where clauses are unilaterally imposed by one party, and it regulates the concept of reasonable compensation in certain mandatory data-sharing scenarios, including specific safeguards in defined SME-related situations. To support implementation,

the European Commission issued non-binding Model Contractual Terms and Standard Contractual Clauses in November 2025 (Chapter IV).

In relation to switching between data processing services (including cloud and edge computing services), providers must:

- allow switching with no more than two months’ notice;
- complete the transition generally within 30 calendar days (subject to exceptions); and
- eliminate switching charges entirely from 12 January 2027, following a transitional cost-based regime (Chapter VI).

Public Sector Access and Third-Country Requests

The Data Act permits public sector bodies to access privately held data only in situations of “exceptional need”, including certain emergencies, and subject to strict requirements of necessity and proportionality (Chapter V). It also establishes safeguards against unlawful access by third-country authorities to non-personal data held in the EU, with implications for contractual arrangements and cloud governance structures (Chapter VII).

Key Organisational Priorities

Organisations should:

- identify whether they qualify as data holders and/or providers of data processing services;
- map “readily available” product/service data;
- implement compliant access and sharing mechanisms;
- align contracts (data-sharing and cloud) with fairness and switching rules;
- update mandatory information and ensure GDPR alignment; and
- document trade secret and non-discrimination safeguards.

3.4 Regulators and Enforcement

ARCEP is the competent authority for enforcing the cloud-related provisions of the SREN Law. It has investigative powers, can settle disputes, and may impose fines of up to 3% of worldwide annual turno-

ver (or 5% in the case of a repeat infringement within the statutory period).

Regarding the EU Data Act, a French DDADUE bill currently under parliamentary examination proposes to designate ARCEP as the competent authority for enforcement, with the exception of Chapter VII. At the time of writing, this bill has not yet been adopted.

The CNIL remains the supervisory authority for GDPR matters. For example, if a cloud-switching failure results in a personal data breach, the CNIL is competent for the GDPR aspects (eg, security and breach notification), while ARCEP may address any breach of cloud-switching obligations within its remit.

The SREN Law establishes co-ordination mechanisms – ARCEP must consult the CNIL for certain decisions concerning data intermediation services involving personal data and must refer suspected anti-competitive practices in cloud markets to the French Competition Authority. These arrangements ensure institutional co-ordination but do not create a unified tripartite regulatory regime.

4. Sectoral Topics

4.1 Use of Cookies

Legal Framework: ePrivacy Implemented in France

In France, the placement or reading of cookies and similar trackers on a user's terminal equipment is governed by the ePrivacy framework (Directive 2002/58/EC, Article 5 (3)) as implemented by Article 82 of the French DPA. As a rule, storing or accessing information on a device requires the user's prior informed consent, unless a narrow exemption applies (eg, trackers that are "strictly necessary" for providing a service are expressly requested by the user or required to enable core site functionality).

Consent Standard and Practical Design

CNIL guidance has established demanding expectations for consent interfaces: users should be able to refuse as easily as accept; consent must be specific and granular; and withdrawal must be possible at any time with an effect comparable to refusal. Organisations must also be able to evidence consent, docu-

ment retention periods, and manage third-party trackers through contract and technical controls (eg, a consent management platform, tag governance, and auditing).

Cookie Walls and Conditional Access

Following French and EU case law developments, cookie walls are not automatically unlawful, but they raise a high bar: the user must have a genuine, free choice and must not be coerced into consenting, taking into account the service's market position and the availability of alternatives. In practice, many services in France avoid blanket "take it or leave it" consent models and implement alternatives (eg, contextual advertisements, paid access, or reduced tracking options), coupled with clear information.

Enforcement Exposure

Cookies and tracking remain one of the CNIL's highest enforcement priorities, including for foreign platforms targeting French users. This means that even technically "minor" consent design issues (lack of prominence symmetry between options, unclear purposes, or continued reading of cookies after withdrawal) can lead to significant regulatory risk.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised or targeted advertising is regulated through a combination of the GDPR (eg, legal basis and restriction on profiling where it is associated with automated decision-making), the ePrivacy Directive (consent for trackers and electronic marketing), and the new DSA/SREN Law transparency rules.

Profiling Restrictions

Article 22 of the GDPR strictly regulates decisions based solely on automated processing, particularly profiling, when they produce legal effects or have similar significant impacts on an individual. As a rule, every person has the right not to be subject to such automated decisions. Exceptions apply only when the decision is necessary for a contract, authorised by EU or member state law, or based on the individual's explicit consent. In these cases, the controller must implement safeguards, including human intervention, the possibility to present one's viewpoint, and the right to contest the decision. Moreover, automated

decisions cannot rely on sensitive data unless very specific legal conditions are met, and reinforced protective measures are in place.

In addition, the SREN Law and DSA prohibit the presentation of advertisements based on profiling using special categories of personal data (eg, political opinions, health). Targeting minors with profiling-based ads is also strictly banned.

Transparency

Under the DSA, online platforms must ensure advertisements are clearly identifiable and provide, directly from the advert itself, meaningful information about the main parameters used to determine why the recipient is being shown the ad, and where applicable, information on how to change those parameters.

Direct Marketing

Under Article L 34-5 of the CPCE, electronic marketing (email, SMS) requires prior opt-in consent, unless the recipient is an existing customer for similar products/services or is a professional (B2B) being contacted on a work address.

4.3 Employment Privacy Law

In France, there is no single “employment privacy act”. Employment privacy is governed by the GDPR and the FDPA, overseen by the CNIL. Importantly, it is also framed by French Labour Code rules (notably proportionality and information/consultation requirements). For instance, the Labour Code expressly states that no personal information may be collected through a device that has not been brought to the employee’s attention beforehand, and the employees’ representative body (*Lecomité social et économique* – CSE) must be informed/consulted in advance on employee monitoring tools and methods.

Key Themes Related to Privacy in the Workplace

Employee monitoring

Monitoring (eg, time tracking, CCTV, IT logs, geolocation) must be necessary, proportionate and disclosed. For vehicle geolocation, the CNIL indicates that the employer should not track outside working time and information collected should not be used to calculate working time when another method already exists. A CNIL fine published on 4 February 2025 (“inactivity”

scoring, frequent screenshots, permanent filming) shows where monitoring crosses the line, and high-risk/constant monitoring may trigger a DPIA.

Remote work

Remote work is defined in Labour Code Article L1222-9 and is usually set by a collective agreement or, failing that, an employer charter after consulting the CSE; it may also be agreed individually. The CNIL highlights reinforced security for telework and configuring tools to minimise data collected.

Communication tools at work

The CNIL notes that employers may control internet and email use for security and policy enforcement but must set rules and inform employees (often via an IT charter). For bring your own device (BYOD), the CNIL recommends separating professional from private spaces; remote wiping should be limited to the professional space, not the whole personal device.

Recruitment

The CNIL’s guide requires collecting only data that is strictly necessary to assess candidates, providing GDPR notices, and defining retention. The CNIL indicates that an unsuccessful candidate’s file may be kept for a short period (eg, up to about three months) to manage feedback/contestation, and then up to two years after the last contact only if the candidate is clearly informed and has agreed or can easily object. Background checks must be job-relevant – a criminal record extract (Bulletin No 3) may be requested only in limited, justified cases and should be consulted but not retained; where an authority grants approval, that approval generally suffices.

4.4 Data Protection in M&A

Under the EU GDPR and the FDPA, there is no “M&A carve-out” – any disclosure, transfer and reuse of personal data must be lawful, transparent, proportionate and secure. The following key principles must be followed:

- Due diligence/data room – disclose only what is necessary (data minimisation), and use strict access controls, logging and NDAs; avoid special-category data unless strictly needed.

- Controller/processor set-up – the main parties (auditor and auditee) are usually independent controllers during diligence. However, the due diligence process typically involves data processors, such as electronic data room providers. A data processing agreement compliant with Article 28 of the GDPR must be concluded with such entities.
- Change of control/transparency – when the buyer becomes the new controller, they must provide updated privacy information; where data is obtained indirectly, Article 14 information must be given “as soon as reasonably possible” and at the latest, within one month (subject to limited exceptions).
- Post-closing integration – reassess purpose compatibility, retention, security, contracts, and cross-border transfer safeguards before merging datasets.

5. International Considerations

5.1 Restrictions on International Data Transfers

France adheres to Chapter V of the GDPR regarding international transfers of personal data. Transfers of personal data outside the EEA are prohibited unless the destination country ensures an adequate level of protection.

- Adequacy decisions: Transfers to countries with an EU adequacy decision (eg, Japan, UK and USA under the Privacy Framework) are unrestricted.
- Appropriate safeguards: For other countries, organisations must use tools like the European Commission’s standard contractual clauses (SCCs) or binding corporate rules (BCRs).
- Transfer impact assessments (TIAs): Organisations must conduct a TIA to verify if the laws of the recipient country (especially regarding government surveillance) impinge on the effectiveness of the safeguards (ie, this does not concern transfers based on adequacy decisions). In January 2025, the CNIL published a comprehensive guide on TIAs, outlining a five-step methodology for this assessment.

5.2 Government Notifications and Approvals No General Prior Approval for GDPR Transfers

France does not impose a general government notification or approval requirement for transfers of personal data outside France or the EEA beyond the GDPR mechanisms (adequacy, Article 46 safeguards, or Article 49 derogations). In practice, organisations are expected to self-assess document compliance, and the CNIL may review transfer arrangements in audits or investigations.

Sector-Specific or Secrecy-Driven Constraints

Certain categories of information (eg, defence secrets, classified information, certain regulated critical infrastructure data, professional secrecy such as legal privilege or banking secrecy) may be subject to separate restrictions with regard to disclosure abroad, which operate independently from GDPR transfer rules. These restrictions are case-specific and typically arise from national security law, public law, criminal law or professional regulations rather than from data protection statutes as such.

Non-Personal Data: EU Data Act Context

The EU Data Act (Article 32) sets safeguards against third-country government access to or transfer of non-personal data held in the EU by providers of data processing services. Providers must take adequate technical, organisational and legal (including contractual) measures to prevent such access/transfer where it conflicts with EU or member state law. Third-country decisions requiring access/transfer are enforceable only if based on a relevant international agreement (eg, a mutual legal assistance treaty or MLAT); otherwise, and where compliance would risk such a conflict, access/transfer may occur only under specified procedural conditions, with data minimisation and (generally) customer notification.

5.3 Data Localisation Requirements No General Localisation Rule

French law does not impose a broad requirement to store personal data in France. Under the GDPR, localisation may be relevant as a risk mitigation measure (eg, to limit international transfers) but is not mandated as such.

Sectoral and Contractual Localisation Drivers

France enforces data localisation for specific strategic sectors.

Health data

Electronic health data must be hosted by a certified health data hosting (*hébergeurs de données de santé* or HDS) provider. While the law allows hosting within the EEA, there is a strong policy push for hosting in France or on sovereign cloud infrastructures.

SecNumCloud

The “*Cloud de Confiance*” doctrine promotes the use of cloud services qualified by ANSSI (SecNumCloud) for public administrations and essential operators (*Opérateur d’Importance Vitale/Opérateur de Services Essentiels* – OIV/OSE). This qualification imposes strict immunity from extraterritorial laws (like the US CLOUD Act), effectively requiring data to be stored and processed within the EU by entities that are not subject to non-EU jurisdiction.

5.4 Blocking Statutes

France has a long-standing blocking statute (Law No 68-678 of 26 July 1968, as amended). Subject to international treaties or agreements, it restricts the communication of certain economic information to foreign public authorities and, more broadly, the gathering/communication of such information for use as evidence in foreign judicial or administrative proceedings.

Covered Information

The statute applies to documents or information of an economic, commercial, industrial, financial, or technical nature where disclosure is likely to harm France’s sovereignty, security, essential economic interests, or public order.

Personal data is not singled out as a standalone category in the law, but datasets that include personal data (eg, customer files) can be treated as covered when they qualify as economic/commercial/technical information and meet the “harm” threshold.

Enforcement Mechanism (SISSE – Since 1 April 2022)

Since 1 April 2022, a decree has designated the Strategic Information and Economic Security Service (SISSE) as the “single point of contact” for notifications. Organisations receiving (i) a request from a foreign public authority to communicate potentially covered information, or (ii) a request relating to the constitution of evidence for foreign proceedings, must notify SISSE without delay and may obtain an administrative opinion on whether Articles 1 and/or 1 bis apply.

Criminal Penalties

Breaches of Articles 1 or 1 bis of the law are criminal offences punishable by up to six months’ imprisonment and a EUR18,000 fine (for individuals). For legal entities, the maximum fine is multiplied by five (ie, EUR90,000).

Exceptions/Lawful Disclosure Routes

The statute allows disclosure where an applicable international treaty or agreement provides for it (eg, co-operation/assistance mechanisms). Article 1 bis also operates subject to applicable laws and regulations. There is no general carve-out simply because the recipient is in the EU or because information is “publicly available” (these factors may be relevant factually case by case, but they are not stated as blanket exceptions in the statute).

Interaction With Data Protection

The blocking statute is distinct from the GDPR, but the two can converge in cross-border evidence collection or regulatory investigations that involve personal data. In such contexts, organisations in France need to reconcile multiple constraints: GDPR Chapter V transfer rules, the blocking statute (including SISSE notification/opinion process), professional secrecy (eg, legal privilege), trade secret protection, and sector-specific secrecy obligations (eg, banking secrecy).

5.5 Recent Developments

EU-US Data Privacy Framework (DPF)

In September 2025, the General Court of the EU (*Latombe* case) upheld the validity of the DPF, rejecting a challenge by a French parliamentarian. This provides renewed stability for transfers to certified

US companies, although privacy advocates remain vigilant.

CNIL International Strategy 2025–2028

The CNIL has adopted a strategy aimed at strengthening European co-operation (including more efficient handling of cross-border cases) and promoting high data protection standards internationally through what it refers to as “data diplomacy”.

New Adequacy Developments – Brazil

In January 2026, the EU and Brazil concluded adequacy arrangements intended to facilitate secure and free data flow between the EU and Brazil. This reduces the need for SCCs or BCRs for transfers covered by the decision.

Anticipated Developments

UK adequacy decision

The EU adequacy decisions for the UK were renewed in December 2025 for a further six-year period (until 27 December 2031), subject to a “sunset clause” and ongoing monitoring. While transfers may continue without additional safeguards, divergence between UK and EU data protection law remains a structural risk that organisations should monitor.

Digital sovereignty and sector-specific localisation trends

Discussions on digital sovereignty and strategic autonomy continue at EU and member state level. While the GDPR does not impose a general data residency requirement, sector-specific rules, certification schemes, or public procurement conditions may increasingly influence expectations regarding localisation or EU-controlled processing in sensitive sectors. At present, however, this remains policy-driven and context-dependent rather than a generalised legal obligation under Chapter V of the GDPR.

GREECE

Law and Practice

Contributed by:

Natasha Mezini, Lambros Katsiamagkos and Jenny Georgountzou
Psarras, Georgountzou - GKP Law Firm



Contents

1. Legal and Regulatory Framework p.131

- 1.1 Overview of Data and Privacy-Related Laws p.131
- 1.2 Rights and Obligations p.132
- 1.3 Special Categories of Personal Data p.133
- 1.4 Processing of Personal Data for Research and Development Purposes p.134
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.135
- 1.6 Data Breach Requirement p.136
- 1.7 Regulators p.137
- 1.8 Enforcement Proceedings and Fines p.138
- 1.9 Enforcement Trends p.139

2. Privacy Litigation p.139

- 2.1 Privacy Litigation Overview p.139
- 2.2 Recent Case Law p.140
- 2.3 Collective Redress Mechanisms p.140

3. Requirements for the Protection and Processing of Non-Personal Data p.141

- 3.1 Objectives and Scope of Data Regulation p.141
- 3.2 Interaction of Data Regulation and Data Protection p.143
- 3.3 Rights and Obligations Under Applicable Data Regulation p.143
- 3.4 Regulators and Enforcement p.144

4. Sectoral Topics p.144

- 4.1 Use of Cookies p.144
- 4.2 Personalised Advertising and Other Online Marketing Practices p.145
- 4.3 Employment Privacy Law p.146
- 4.4 Data Protection in M&A p.146

5. International Considerations p.146

- 5.1 Restrictions on International Data Transfers p.146
- 5.2 Government Notifications and Approvals p.148
- 5.3 Data Localisation Requirements p.148
- 5.4 Blocking Statutes p.148
- 5.5 Recent Developments p.148

Psarras, Georgountzou - GKP Law Firm has ten lawyers at its offices in Athens, and an effective network of other lawyers throughout Greece. The firm is well established in all areas of regulation, especially in corporate law, finance, banking, employment, IT, energy, media and pharma, as well as real property and construction. GKP advises mainly foreign companies active in Greece through a subsidiary or a branch office, or on a project basis, on negotiating, contract-

ing and monitoring the performance of contracts or investments in Greece, in the public or private sector, including M&A. The firm has assisted in the setting up of distribution networks in various fields (vehicles, IT, food and drink, pharma) and has vast experience in all aspects of commercial law, especially agency, distribution and franchising, including an excellent track record in IP and competition law issues.

Authors



Natasha Mezini specialises in commercial law, intellectual property, competition law and the law of new IT technologies. She advises clients on compliance issues related to personal data, privacy, minors' personal data,

special categories of data in the healthcare and pharmaceutical industries, and electronic communications. Natasha is also a certified Data Protection Officer, and has contributed to Lexology publications on Data Protection & Privacy (2023) for Greece. She graduated from the University of Thessaloniki, Law School (LLB) and the University of Piraeus (MSc) in Law, IT and Communications Technologies, and the University of Athens Law School (LLM). Natasha speaks Greek and English.



Lambros Katsiamagkos is a senior associate specialising in regulatory compliance, including personal data protection and privacy. He participated in consulting for the Ministry of Development on the

evaluation of the Greek regulatory environment and the simplification of the business licensing procedures by the World Bank in 2013, and for the OECD on the simplification of the business licensing procedure. He advises clients on corporate, employment and criminal law, and represents them before the national courts and international arbitral tribunals. He is a graduate of the University of Luton, UK (LLB) and the University of Athens, Law School (LLB), and speaks Greek, English and German.



Jenny Georgountzou is the managing partner of GKP and specialises in regulatory compliance, including personal data protection and privacy. She has participated in multinational data protection compliance projects,

data training and awareness exercises, and assists clients with security and compliance issues, regulatory filings, notifications, data breach incidents, processing special categories of personal data, drafting policies, cross-border data transfers and marketing communications. Jenny also advises on corporate law, agency and distribution, franchises, and intellectual and industrial property rights, and represents clients before the national courts and international arbitral tribunals. She is admitted to the Supreme Court of Greece and speaks Greek, English and French.

Psarras, Georgountzou - GKP Law Firm

8, Karneadou Street
Athens
106 75
Greece

Tel: +30 2107 2172 32
Fax: +30 2130 9939 65
Email: georgountzou@gkplaw.gr
Web: www.gkplaw.gr



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The fundamental provisions for privacy and data protection in Greece are as follows, in order of priority.

Regulation (EU) 2016/679

Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (GDPR) is the main legislation for the protection of personal data. The GDPR is directly applicable in Greece and supersedes any provision of national law, including the Constitution. The GDPR provides for the imposition of penalties (Article 83) and the obligation to compensate for damages incurred (Article 82) in case of violation of its provisions.

Constitution

The Greek Constitution sets out the basic principles for the privacy of communications and the protection of personal data.

- Article 9A of the Constitution establishes protection from the processing, collection and use of personal data, and provides for establishing an independent authority to safeguard such rights. In 1997, the Hellenic Data Protection Authority (HDPa) was established according to Law 2472/1997.

- Article 19 of the Constitution establishes the privacy of correspondence (namely post/mail, which is the oldest form) and the freedom of communications in general, and provides for establishing an independent authority to safeguard such rights. In 2003, the Hellenic Authority for Communications Security and Privacy was established according to Law 3115/2003.

Civil Code

Articles 57–59 of the Greek Civil Code include fundamental provisions for protecting the individual's personality. An offence to the individual's personality may substantiate civil claims for injunction, compensation and moral damages.

Laws

- Law 4624/2019 provides the necessary measures for the implementation of the GDPR and transposes the provisions of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Moreover, Law 4624/2019 includes provisions for the operation of the HDPa.
- Law 2472/1997 transposes Directive 95/46/EC on the protection of individuals with regard to the pro-

cessing of personal data, and applies to the extent that a few of its articles remain in force.

- Law 3471/2006 provides for the protection of privacy and personal data in electronic communications.
- Law 3674/2008 provides for the necessary measures that must be applied by the providers of electronic communications networks and services to safeguard the safety and privacy of communications.
- Law 3917/2011 transposes the provisions of Directive (EU) 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.
- Law 4727/2020 transposes the provisions of Directives (EU) 2016/2102, 2019/2024 and 2018/1972 on electronic communications.
- Law 5002/2022 on the privacy of communications and cybersecurity aims to protect the confidentiality of communications from surveillance and monitoring.
- Law 5086/2024 establishes the National Cybersecurity Authority.
- Law 5099/2024 incorporates Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (the Digital Services Act) and designates the HDPA as the competent authority for supervising providers of intermediary services, enforcing Article 26 paragraphs 1 and 3 of the Regulation regarding user information on the display and targeting of advertisements, and Article 28 concerning the protection of minors' personal data.
- Law 5160/2024 incorporating Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2).
- Law 5169/2025 ratifying the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of personal data.
- Regulatory acts and guidelines issued by the competent authorities.

- Lastly, the competent, independent authorities, such as the HDPA and the Hellenic Authority for Communication Security and Privacy, issue regulatory acts and guidelines.

1.2 Rights and Obligations

GDPR General Principles

The GDPR sets the following general principles for the processing of personal data, which safeguard the fundamental rights of the natural persons, including their protection from the processing of their personal data:

- “lawfulness, fairness and transparency” – the processing of personal data must be lawful, legitimate and carried out in a transparent manner;
- “purpose limitation” – personal data must be collected for an explicit, specified and legitimate purpose and the processing must be compatible with such purpose;
- “data minimisation” – personal data must be adequate, relevant and limited to what is strictly necessary for the fulfilment of the purpose for which it is processed;
- “accuracy” – personal data must be accurate and kept up to date, and measures must be taken to rectify inaccurate data;
- “storage limitation” – personal data must be retained only for as long as necessary to fulfil the purpose of processing; and
- “integrity and confidentiality” – personal data must be processed securely and in a manner that protects it against unauthorised or unlawful processing, loss or destruction.

Data Subjects' Rights

Chapter II of the GDPR sets out the rights of data subjects, which safeguard their fundamental freedoms regarding the processing of their personal data:

- Article 15 establishes the right of access, meaning that the data subject has the right to obtain confirmation from the data controller as to whether or not their personal data is being processed and, if so, to access such personal data and receive a copy thereof;
- Articles 16 and 17 establish the right to rectification or erasure, meaning that the data subject may request the correction of their personal data that

- is inaccurate or incomplete, and/or the deletion of his/her personal data, provided the request is lawful and there are no overriding legitimate grounds for the processing;
- Article 18 establishes the right to the restriction of processing, meaning that the data subject may request the suspension of processing, provided the request is lawful;
 - Article 20 establishes the right to data portability, meaning that the data subject may request and receive a copy of their personal data in a structured, commonly used and machine-readable format, and/or request their transmission to another data controller; and
 - Article 21 establishes the right to object, meaning that the data subject may object to the processing of their personal data, provided the request is lawful.

Compliance Checklist for Data Controllers

The GDPR and Greek Law 4624/2019 set out the conditions under which entities/organisations may process personal data. Entities/organisations acting as data controllers must meet the following compliance requirements.

- Mapping processing activities.
- Providing information to data subjects regarding:
 - (a) the type and nature of personal data collected and processed;
 - (b) the purposes of the processing of personal data;
 - (c) the legal basis on which the processing of personal data is carried out;
 - (d) the retention period of the personal data;
 - (e) the rights of data subjects and how these rights may be exercised;
 - (f) whether the data subject is subject to automated decision-making (profiling); and
 - (g) the recipients or third parties to whom personal data are transferred.
- Drafting and publishing privacy policies (employee privacy policy, CCTV policy, website cookies policy, vendors' privacy policy, etc).
- Collecting consent from data subjects where required (eg, sending newsletters for marketing purposes, cookies, processing special categories of data).

- Concluding data processing agreements with processors or third parties to whom personal data is transferred, in order to ensure transparency and the lawfulness of processing by third parties.
- Performing a Data Protection Impact Assessment (DPIA) when there is a high risk to the rights and freedoms of data subjects or when processing is carried out on a large scale.
- Implementing appropriate technical and organisational security measures, such as:
 - (a) access control;
 - (b) encryption;
 - (c) pseudonymisation;
 - (d) data back-ups;
 - (e) strong password policies;
 - (f) security incident management;
 - (g) incident response plan for personal data breaches; and
 - (h) procedure for notifying the HDSA and data subjects of personal data breaches.
- Training staff and raising awareness on the basic principles of the GDPR, the secure handling of personal data and the application of the privacy policies adopted.
- Continuously monitoring legislation and regularly reviewing and updating the privacy policies and technical and organisational security measures adopted.

1.3 Special Categories of Personal Data

According to Article 9 of the GDPR and Law 4624/2019, special categories of personal data include data relating to:

- racial/ethnic origin;
- political opinions;
- religious/philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for identification;
- health data; and
- sex life or sexual orientation.

Processing the special categories of personal data is prohibited, and is permitted only if:

- the data subject has given his/her explicit consent for the processing;

- the processing is necessary for carrying out the obligations and exercising specific rights of the data controller or the data subject in the field of employment, social security and social protection law, including pensions in accordance with applicable law;
- the processing is necessary for the protection of the vital interests of the data subject or another natural person, where the data subject is physically or legally incapable of giving his/her consent;
- the processing takes place within the legitimate activities of a non-profit entity/organisation with a political, philosophical, religious or trade union purpose, provided the processing regards only its members or former members and the personal data is not disclosed outside the entity/organisation;
- the processing is of personal data that has been manifestly made public by the data subject (eg, online posts, social media, interviews, publications);
- the processing is necessary for the establishment, exercise or defence of legal claims, or when courts act in their judicial capacity;
- the processing is necessary for reasons of substantial public interest;
- the processing is necessary for preventative or occupational medicine;
- the processing is necessary for public health purposes; or
- the processing is necessary for archiving purposes in the public interest, scientific or historical research, or for statistical purposes.

Personal Data Relating to Minors

Minors enjoy special protection as they are not aware of the risks involved in the processing of their personal data. Minors can consent to the processing of their personal data if they are at least 16 years old and the data controller uses clear, accurate and simple language to inform the minors prior to obtaining their consent.

When it comes to the internet and the provision of services to minors, minors can consent to the processing of their personal data if they are at least 15 years old. If minors are under this age, the consent must be granted by their legal representative – ie, parent or

legal guardian. Decisions based solely on automated processing are prohibited, where such decisions legally affect or influence significantly minors. Profiling for promotional or marketing purposes is prohibited.

Personal Data Relating to Criminal Convictions

Greek Law 4624/2019 – which transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data – provides the general principles and requirements for the processing of personal data relating to criminal convictions and offences by police, prosecutors and judicial authorities for criminal law enforcement purposes. Personal data relating to criminal convictions and offences constitutes a separate category of personal data, which may be processed only under the control of an official authority, when it is absolutely necessary for the performance of the duties of the data controller and with the application of appropriate safeguards for the rights and freedoms of the data subjects.

1.4 Processing of Personal Data for Research and Development Purposes

Health data is one of the special categories of personal data whose processing can take place under the requirements described in 1.3 Special Categories of Personal Data. According to Article 30 of Greek Law 4624/2019, by derogation to the above, health data can be processed for scientific purposes, including research and development, without the consent of the data subject, provided:

- the interest of the controller exceeds the interest of the data subject not to have his/her personal data processed; and
- the controller takes appropriate measures for the protection of the legal interests of the data subject, which may include:
 - (a) limiting access to the personal data for the controller and processors;
 - (b) pseudonymising personal data;
 - (c) encrypting personal data; and

- (d) appointing a DPO.

In view of the above, companies that provide products or services to healthcare providers may anonymise patient personal data for the purposes of product development or scientific research.

Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space (EHDS) entered into force in March 2025 and aims to establish a common framework for the use and exchange of electronic health data across the EU. It strengthens individuals' access to and control over their personal electronic health data, while also allowing the further use of certain data for purposes of public interest, policy support and scientific research. It promotes a data environment specifically tailored to health, and supports the single market for digital health services and products. In addition, the Regulation establishes a harmonised legal and technical framework for Electronic Health Record (EHR) systems, enhancing interoperability, innovation and the smooth functioning of the internal market.

The EHDS Regulation will:

- enable individuals to access, control and exchange their electronic health data across borders for the provision of healthcare;
- allow the secure and trustworthy re-use of health data for research, innovation, policymaking and regulatory activities; and
- promote a single market for electronic health record systems, supporting both primary and secondary uses of data.

Chapter IV of the EHDS Regulation sets out the conditions for the so-called "secondary use" of health data, including the use of personal data for research and development purposes. The data access bodies indicated by the member states shall grant access to electronic health data for secondary use when the processing of such health data is necessary for any of the following purposes:

- the public interest in the domain of public health;

- policy making and regulatory activities in the public sector;
- statistics;
- education or teaching activities in the sectors of health or care;
- scientific research and improvement in the fields of health or care, with the aim of benefiting end users such as patients, healthcare professionals and health system managers – this includes:
 - (a) development and innovation activities for products or services; and
 - (b) training, testing and evaluating algorithms, including those used in medical devices, in vitro diagnostic medical devices, AI systems and digital health applications.

Health data provided for the above purposes shall be limited to what is absolutely necessary, adequate and relevant to the purpose of the processing. Health data shall be provided in an anonymised format; if the specific processing cannot be achieved with anonymised data, then health data shall be provided in a pseudonymised format, while access to the information necessary to reverse the pseudonymisation shall be restricted and controlled.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Regulation (EU) 2024/1689, known as the AI Act, establishes harmonised rules on artificial intelligence and represents the first comprehensive legal framework for AI worldwide. It covers AI systems' development, marketing, deployment and use. In Greece, there have been no recent legislative updates concerning the regulation of artificial intelligence that would affect data protection. Existing data protection laws continue to apply directly to the safeguarding of personal data, even in the context of using AI systems.

The AI Act does not seek to affect:

- the application of existing EU law governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments;
- the obligations of providers and deployers of AI systems in their role as data controllers or proces-

sors stemming from EU or national law on the protection of personal data insofar as the design, development or use of AI systems involves the processing of personal data; nor

- the rights and guarantees awarded to data subjects by such EU law, including the rights related to solely automated individual decision-making, including profiling.

On the contrary, the AI Act should facilitate the effective implementation and exercise of the data subjects' rights and other remedies guaranteed under EU law on the protection of personal data.

There are no specific laws regarding AI in Greece that relate to or affect the protection of personal data.

The reliance of AI technologies on large datasets can create significant privacy risks. AI systems are often trained on vast amounts of personal information, sometimes collected without proper consent, or used in ways that individuals might not expect. This can lead to unintended consequences, such as exposing sensitive personal details or allowing for intrusive profiling. For example, an AI model used to predict consumer preferences might draw on data from social media, shopping history or even biometric information, potentially leading to privacy violations, if such data is mishandled or shared without adequate safeguards.

To address the above risks and harness the benefits of AI responsibly, the EU has embarked on regulatory initiatives aimed at balancing innovation with the protection of fundamental privacy rights. Personal data protection legislation plays a vital role, as AI systems are often built on personal data and rely on it. Therefore, personal data principles and requirements help to address some of the above risks.

To support data protection professionals, the HDPa provides relevant training material developed by external experts of the EDPB under the supervision of the HDPa's specialised scientific staff, which consists of two complementary training programmes, each accompanied by interactive comprehension and self-assessment questions about the use of AI systems.

1.6 Data Breach Requirement

A personal data breach (Article 4 (12) of the GDPR) is defined as a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. According to the Guidelines 18/2018 of the Article 29 Working Party (now the European Data Protection Board) on personal data breach notification ("Guidelines on Personal Data Breach Notification under Regulation 2016/679", WP 250 rev.1), one category of personal data breach is based on the security principle of confidentiality, which occurs when there is unauthorised access to personal data ("confidentiality breach").

A breach may potentially have various significant adverse effects on individuals, which may lead to physical, material or non-material damage. The GDPR explains that such damage may include loss of control over personal data, limitation of rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, reputational harm, or loss of confidentiality of personal data protected by professional secrecy, among others.

In the case of a data breach, the data controller must comply with the following obligations.

Assess the Data Breach Without Undue Delay

The data controller must determine:

- what happened and when;
- which data was affected;
- how many data subjects are impacted;
- the likely consequences; and
- whether the breach poses a risk or high risk to data subjects.

The above assessment must be documented.

File a Notification With the HDPa

If the breach is likely to result in a risk to the rights and freedoms of the individuals, the data controller must notify the breach to the HDPa within 72 hours of becoming aware of such breach. The HDPa has an online form, which must be completed and filed by the data controller, including information on the nature of the breach, the categories of personal data affected,

the number of the individuals affected, the mitigation measures implemented, the contact details of the data controller, etc. Any delay in filing the above notification with the HDPa must be justified.

Communicate the Breach to Affected Individuals

If the breach is likely to result in a high risk to the rights and freedoms of the individuals, the data controller must inform the individuals about such breach immediately and without undue delay, in clear and plain language, explaining:

- the nature of the breach;
- the potential consequences;
- the contact details of the data controller; and
- the mitigation measures implemented or suggested.

Communication may be avoided only in limited cases – eg, where data was encrypted and not readable to third parties without authorisation, or if any risk has been fully mitigated.

Maintain an Internal Breach Register

All breaches – even those not notified – must be recorded with details of facts, effects and remedial actions.

1.7 Regulators

The Hellenic Data Protection Authority (HDPa)

The HDPa has control powers, as well as corrective, advisory and licensing powers, as specified and described in Article 58 of the GDPR and Article 15 of Law 4624/2019. Analytically, the HDPa:

- monitors the implementation and enforcement of the GDPR, Law 4624/2019 and other regulations concerning the protection of individuals from the processing of personal data;
- contributes to the consistent application of the GDPR throughout the European Union and, for this purpose, co-operates with the supervisory authorities of the EU member states and with the Commission;
- promotes public awareness of personal data protection issues and the obligations of controllers and processors;

- provides opinions on any regulation to be included in a law or regulatory act concerning data processing;
- issues instructions and makes recommendations on any matter concerning data processing;
- provides, upon request, information to data subjects regarding the exercise of their rights;
- handles complaints submitted for violation of the provisions of the GDPR;
- conducts investigations or audits regarding the implementation of personal data protection legislation;
- encourages the development of codes of conduct and approves codes of conduct that provide adequate safeguards;
- encourages the establishment of data protection certification mechanisms and data protection seals and marks, and approves certification criteria;
- co-operates with other supervisory authorities through the exchange of information, aiming for a more consistent application of the GDPR throughout the EU; and
- contributes to the activities of the EDPB.

The Hellenic Authority for Communication Security and Privacy (ADAE)

The ADAE is responsible for monitoring the implementation of all legislation relevant to the lawful interception of communications. Analytically, the ADAE:

- issues regulations regarding the assurance of the confidentiality of communications;
- performs audits on communications network/service providers, public entities and the Hellenic National Intelligence Service, and holds respective hearings;
- investigates relevant complaints from members of the public; and
- collects relevant information using special investigative powers.

The Hellenic Cybersecurity Authority (NCSA)

The NCSA aims to organise, co-ordinate and implement a comprehensive framework of strategies, measures and actions for achieving and maintaining a high level of prevention, protection, deterrence, response and recovery from cyber-attacks. Analytically, the NCSA:

- monitors and supervises the implementation of the EU Directive on measures for a high common level of cybersecurity across the EU (NIS2) in Greece;
- sets the regulatory framework for the operation of critical infrastructure digital systems in Greece;
- supports scientific research, innovation and investments in cybersecurity, contributes to the development of national and international standards, and promotes education and awareness in the field;
- is the designated single point of contact for reporting security incidents and may intervene to assist in the management of such incidents; and
- co-operates with national and international authorities to exchange information and best practices.

1.8 Enforcement Proceedings and Fines Enforcement Proceedings

Enforcement proceedings before the HDPa are governed by the provisions of Law 3051/2002 and the Code of Administrative Procedure. Decision No 9/2022 of the HDPa, as amended, includes the Rules of Operation of the HDPa and provides that every case must follow these basic procedural steps:

- case file preparation before the hearing;
- hearing before the HDPa – the hearings are not open to the public; and
- in the event of reprimand or the imposition of penalties, the HDPa issues its decision only after having heard the parties involved, who may file submissions before the hearing, attend the hearing in person or with an attorney, provide clarifications upon request during the hearing and file closing submissions.

The HDPa examines complaints and conducts investigations or audits either ex officio or following a complaint, in order to ensure compliance with applicable legislation regarding the protection of personal data. In exercising its powers, the HDPa may dismiss applications, inquiries or complaints that are deemed to be manifestly vague, unfounded, abusive or anonymous. The HDPa informs the person who has filed a complaint, and all parties involved, about the actions it takes.

Without prejudice to the deadlines set by the GDPR, the prioritisation of applications, inquiries and com-

plaints is assessed by the HDPa based on the importance and broader public interest of the matter. The HDPa may issue decisions on the merits of the case and provisional decisions with measures applicable until the issuance of its decision on the merits of the case. The HDPa's decisions are binding on its addressees, while its enforceable acts are subject to appeal before the Administrative Courts and to annulment by the Council of State.

Administrative Fines

- For individuals and private entities: according to Article 83 of the GDPR, the HDPa may impose administrative fines of up to EUR10 million on private entities or, in the case of an undertaking, up to 4% of the total worldwide annual turnover.
- For public entities: according to Article 39 of Law 4624/2019, administrative fines imposed by the HDPa upon public entities are limited to the amount of EUR10 million.

In 2023, 1,414 recourses/complaints were filed with the HDPa, and penalties totalling EUR637,000 were imposed by way of 27 decisions.

According to Article 83 of the GDPR, when imposing an administrative fine and determining its amount, the HDPa takes the following factors into account:

- the nature, gravity and duration of the violation, considering the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered;
- the intentional or negligent character of the violation;
- any actions taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor, taking into account the technical and organisational measures implemented;
- any relevant previous violations by the controller or processor;
- the degree of co-operation with the HDPa to remedy the infringement and mitigate its possible adverse effects;
- the categories of personal data affected by the violation;

- the manner in which the HDPa became aware of the violation, particularly whether and to what extent the controller or processor notified it;
- compliance with measures previously ordered under Article 58 (2) concerning the same subject matter;
- adherence to approved codes of conduct or approved certification mechanisms; and
- any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, as a result of the infringement.

The HDPa has recently issued decisions imposing significant administrative fines for violations of data protection legislation.

- Decision No 44/2025 imposed an administrative fine of EUR10,000 and EUR80,000 upon an energy provider and call centre in its capacity as data processor, for making telephone calls promoting products and services to individuals who had expressly requested not to receive such calls.
- Decision No 42/2025 imposed an administrative fine of EUR30,000 on an energy services company for violating data subjects' rights of access, rectification and erasure of their personal data.
- Decision No 38/2025 imposed an administrative fine of EUR10,000 on a Municipality for operating a CCTV surveillance system at a vehicle depot without proper notification to the data subjects.

Criminal Penalties

Greek Law 4624/2019 provides for imprisonment and criminal penalties ranging between EUR100,000 and EUR300,000 for the violation of the legislation for the protection of personal data.

1.9 Enforcement Trends

The current most significant enforcement trends in Greece revolve around the following three pillars.

Ex Officio Audits of Surveillance Systems

The HDPa has initiated an audit ex officio on the software developed and installed by the Ministry of Migration and Asylum at the reception and hospitality structures for third-country nationals located at the borders of Greece. The software programs provided for:

- digital management of the electronic and physical security of the above structures with the use of CCTV, drones and artificial intelligence behavioural analytics; and
- control of the persons entering and exiting the above structures, including personnel, third-country nationals seeking asylum and representatives of NGOs, with the use of RFID in combination with two-factor authentication processing biometrical data.

The HDPa attested many violations, including:

- failure to define an appropriate legal basis for the processing of personal data, much of which belongs to the special categories;
- providing deficient information to data subjects prior to the processing;
- inadequate and deficient data processing agreements with the data processors;
- failure to keep a registry of processing activities; and
- failure to perform an appropriate DPIA.

The HDPa imposed an administrative fine of EUR175,000 on the Ministry of Migration and Asylum (Decision No 13/2024).

Implementation of Appropriate Technical and Organisational Measures and Data Breaches

The HDPa has imposed administrative fines for failure to apply appropriate technical and organisational measures, resulting in data breaches from an insider threat (Decision Nos 7/2025, 33/2025).

Violation of Data Subjects' Rights

The HDPa steadily reviews complaints and applies administrative penalties in case of violation of data subjects' rights to access, rectification, erasure and restriction of their personal data (Decision No 1/2025).

2. Privacy Litigation

2.1 Privacy Litigation Overview

The violation of privacy legislation may cause damages, and the affected party has the right to request compensation for material or moral damages from

the data controller or processor. The First Instance Court freely determines the amount of compensation based on the factual circumstances of the case and taking into account all relevant factors, such as the nature and extent of the violation, the degree of fault, the absence of contributory negligence by the data subject, and the financial and social situation of the parties.

Decision No 573/2025 of the Athens Court of Appeal ruled that the unlawful sending of text messages for the purpose of commercial promotion of services established the liability of the sender in his capacity as data controller. Consequently, the data controller was ordered to pay monetary compensation for moral damages to the data subject amounting to EUR10,000 for each text message (SMS).

2.2 Recent Case Law

Article 82 (1) of the GDPR provides that any individual who has suffered material or non-material damage as a result of a GDPR infringement is entitled to compensation. Recitals 75 and 85 of the GDPR list examples of non-material damages, such as loss of control over personal data, restriction of rights, discrimination, identity theft or fraud, unauthorised reversal of pseudonymisation, damage to reputation, loss of data, loss of confidentiality of data and similar harms. Non-material damages may incur when personal data is disclosed or transferred to third parties without the data subject's consent.

In 2021, the CJEU addressed the concept of non-material damages under Article 82 of the GDPR for the first time, in Case C-300/21. More specifically, the harmful conduct of the company consisted in processing the personal data of an individual, which, combined with social or demographic information, led to the identification of that individual with a specific political party. The CJEU clarified the notion of material damage under Article 82 of the GDPR and emphasised the following three requirements for the establishment of the right to compensation in paragraph 36 of its decision:

- the processing of personal data carried out in breach of the provisions of the GDPR;
- the damage suffered by the data subject; and

- a causal link between the unlawful processing and the damage.

Furthermore, in paragraph 59 of the decision, the CJEU stressed that Article 82 of the GDPR must be interpreted as meaning that, for determining the amount of compensation due on the basis of the right established in that article, national courts must apply the domestic rules of each member state concerning the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are respected.

The CJEU has issued case law interpreting Article 82 of the GDPR. In particular, in Case C-655/23, the Court held that Article 82 (1) of the GDPR must be interpreted as meaning that the term “non-material damage” covers the negative emotions experienced by the data subject due to the unauthorised disclosure of their personal data to a third party, such as fear or distress arising from the loss of control over the data, the risk of their potential misuse, or harm to reputation – provided that the data subject demonstrates that these emotions, together with their negative consequences, are causally linked to the infringement of the Regulation.

2.3 Collective Redress Mechanisms

Law 5019/2023 transposes the provisions of Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers. Actions may be brought against infringements by traders of the provisions of the GDPR and Law 3471/2006, among others, for the protection of privacy and personal data in electronic communications. Domestic representative actions can be filed by consumers' unions or organisations, including entities that have been qualified in other member states to bring cross-border representative actions. Consumers' unions or organisations must provide sufficient information about their members/consumers in order for the Court to decide on its jurisdiction and applicable law. The representative action may seek injunctive or redress measures.

In Greece, there is no case law concerning the collective bringing of actions and the awarding of com-

pensation for privacy violations. However, the issue has been addressed by the CJEU, which held in paragraph 32 of Case C-757/22, *Meta Platforms Ireland*, that Article 80 (2) of the GDPR must be interpreted as not precluding national legislation that allows a consumer protection association to bring legal proceedings – without a mandate granted to it for that purpose and irrespective of the existence of an infringement of specific rights of an individual data subject – against an alleged infringer of data protection rules, relying on the violation of the prohibition of unfair commercial practices, the breach of consumer protection legislation or the violation of the prohibition on the use of unfair contract terms, provided that the data processing at issue is capable of affecting the rights conferred on identified or identifiable natural persons by the GDPR.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Regulation (EU) 2018/1807 of the European Parliament and the Council, adopted on 14 November 2018, establishes the principle of the free flow of non-personal data within the EU. Regulation (EU) 2023/2854 of the European Parliament and the Council, adopted on 13 December 2023 and commonly referred to as the Data Act, establishes harmonised rules for fair access to and usage of non-personal data, and sets the rights and obligations of data users, data holders and data processing services. The main objective of the Data Act is to safeguard the fair allocation of the value of the data created from the use of connected products and related services for the benefit of all factors of the digital economy and the promotion of access to data and its use. The Data Act aims to facilitate access to data and the users' open use of data to create a well-functioning internal market for data.

The expanding Internet of Things (IoT), AI and machine learning represent major sources of non-personal data – for example, as a result of their deployment in automated industrial production processes. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to moni-

tor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines. If technological developments make it possible to turn anonymised data into personal data, such data is to be treated as personal data, and the GDPR is to apply accordingly.

IoT

In Greece, Law 4961/2022 introduces for the first time a regulatory framework for the secure use of IoT devices by operators of critical infrastructure in both the public and private sectors. Specifically, the law sets out obligations and compliance declarations for IoT device manufacturers, including the following.

- Cybersecurity measures to be embedded in IoT devices are defined according to their use and the associated security risks, in order to ensure an appropriate level of cybersecurity.
- The minimum content of the manufacturer's declaration of conformity for IoT devices is specified, and such declaration must accompany every device intended to be made available to IoT operators. The law also establishes the manufacturer's obligation to inform all parties involved and the NCSA if the manufacturer becomes aware, by any means, of non-compliance.
- The obligations of importers and distributors of IoT devices are defined, particularly their duties to:
 - (a) verify that the device is accompanied by the declaration of conformity;
 - (b) inform other parties involved and the NCSA if they themselves become aware, by any means, of non-compliance; and
 - (c) maintain a record of notification actions and communicate such record to the NCSA.
- The obligations of IoT operators are set out, including the requirement to appoint an IoT Security Officer, who is responsible for implementing and properly monitoring the technical and organisational measures adopted by the IoT operator to manage risks related to the security of the IoT devices used, and for informing other involved parties and the NCSA if a risk associated with the device's use arises.
- The responsibilities of the NCSA are further specified regarding the assessment and monitoring of compliance by manufacturers, importers, distribu-

tors and IoT operators. In addition, manufacturers, importers and distributors of IoT devices are required to comply with the NCSA's instructions by taking any corrective action necessary to achieve compliance. For the operator using the device, such measures may extend to the suspension of the device's use.

- Given the high risk of disruption to the operation of an IoT device and its potential impact, the law establishes a specific obligation for manufacturers to maintain a process for managing security incidents or vulnerabilities, for each device.
- IoT operators are required to provide users with information about the devices so that each user – regardless of their familiarity with new technologies – can understand basic issues related to the safe installation, configuration and operation of the device.
- Finally, because the processing of personal data within IoT environments may pose a high risk to the rights and freedoms of individuals, IoT operators are required to conduct a DPIA for the planned processing activities related to the operation of IoT devices, in accordance with Article 35 (1) of the GDPR.

Cloud Computing

Cloud computing technology, through which entities and individuals can process and store large volumes of data, creates serious threats to data security and privacy. Law 4727/2020 establishes the government cloud for the public sector (G Cloud) as a set of digital infrastructures managed by the General Secretariat of Information Systems. Government cloud infrastructures also exist in specific public sectors, such as Research and Education (RE Cloud) and the Health Government Cloud (H Cloud). All central electronic applications and central information systems maintained by Ministries, independent authorities and the Information Society are connected to the G Cloud, and they relate to transactions with natural persons, legal entities and public administration.

Although the G Cloud offers significant advantages in terms of flexibility and efficiency, it simultaneously creates serious threats to privacy and personal data protection, because a large volume of citizens' data is stored therein, such as health data. This raises con-

cerns regarding security and confidentiality, especially in the event of a cyber-attack, data breach or violations of personal data.

AI

Regulation (EU) 2024/1689, commonly referred to as the AI Act, establishes harmonised rules on AI and represents the first comprehensive legal framework for AI worldwide. It covers AI systems' development, marketing, deployment and use. In Greece, Law 4961/2022 includes provisions on the use of AI systems in the public sector for decision-making processes that affect the rights of natural persons and legal entities. Public entities that use AI systems are required to carry out a DPIA in accordance with Article 35 of the GDPR and to take the following into account:

- the intended purpose, including the public interest served through the use of the AI system;
- the capabilities, technical characteristics and operating parameters of the AI system;
- the type and categories of decisions made or acts issued with the involvement of the AI system, or supported by it;
- the categories of data collected, processed or entered into the system, or generated by it;
- the risks that may arise for the rights, freedoms and legitimate interests of the natural or legal persons to whom the decision relates or whom it affects; and
- the expected benefit for society as a whole in relation to potential risks and impacts that may result from the use of the AI system, particularly for racial, ethnic, social or age groups and categories of the population such as persons with disabilities or chronic conditions.

Every public entity that uses AI systems must provide specific information to natural persons who are subject to decision-making based on such systems, such as:

- the date on which the AI system began operating;
- the operating parameters, capabilities and technical characteristics of the AI system;
- the categories of decisions made or acts issued with the involvement of the AI system or supported by it; and

- the conduct of an algorithmic impact assessment.

3.2 Interaction of Data Regulation and Data Protection

Regulation (EU) 2018/1807 of the European Parliament and the Council, adopted on 14 November 2018, establishes the principle of the free flow of non-personal data within the EU. Throughout its text, the Regulation uses the term “data”, which is defined as “data other than personal data”. Such data, which is also referred to as “non-personal data”, is inferred a contrario to personal data, as defined in the GDPR. According to the GDPR, “personal data” includes any information relating to an identified or identifiable natural person – ie, the “data subject”. On the contrary, non-personal data can be categorised by origin as:

- firstly, data that originally did not relate to an identified or identifiable natural person, such as data on weather conditions generated by sensors installed on wind turbines or data on maintenance needs for industrial machines; or
- secondly, data that was initially personal data but was later rendered anonymous.

Mixed Datasets

In new technology systems, mixed datasets often appear that consist of both personal data and non-personal data. Mixed datasets represent the majority of datasets used in the data economy and are common because of technological developments such as the IoT (ie, digitally connecting objects), AI and technologies enabling big data analytics. In the case of a dataset composed of both personal and non-personal data, Regulation (EU) 2018/1807 applies to the non-personal data part of the dataset and the GDPR applies to the personal data part of the dataset. Where personal and non-personal data in a dataset are inextricably linked, Regulation (EU) 2018/1807 shall not prejudice the application of the GDPR, meaning that:

- Regulation (EU) 2018/1807 on the free flow of non-personal data applies to the non-personal data part of the dataset;
- the GDPR applies to the personal data part of the dataset; and
- if the non-personal data part and the personal data parts are “inextricably linked”, the data protection

rights and obligations stemming from the GDPR apply fully to the whole mixed dataset, including when personal data represents only a small part of the dataset.

3.3 Rights and Obligations Under Applicable Data Regulation

Access Right

Regulation (EU) 2018/1807 on the free flow of non-personal data within the EU provides that national competent authorities have the right to request or obtain access to data for the purpose of carrying out their official duties in accordance with EU or national law. Providers are not permitted to refuse competent authorities access to data on the grounds that the data has been processed in another member state. If a competent authority does not obtain access following a request for access to a user’s data, that authority may request the assistance of another competent authority from a different member state. Once access to the data and to any equipment or means of data processing is obtained, such access must comply with fundamental principles and with national and European legislation.

Portability Right

Regarding the right to data portability, the Commission encourages the development of self-regulatory codes of conduct at EU level in order to contribute to a competitive data economy in line with the principles of transparency and data interoperability. In particular, Article 6 of the Regulation provides that the following must be ensured:

- best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format, including open standard formats where required or requested by the service provider receiving the data;
- minimum information requirements to ensure that professional users are provided – before a contract for data processing is concluded – with sufficiently detailed, clear and transparent information regarding the processes, technical requirements, timeframes and charges that apply if a professional user wants to switch to another service provider or port data back to its own IT systems;

- approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services – such approaches may include quality management, information security management, business continuity management and environmental management; and
- communication roadmaps taking a multidisciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.

The GDPR and Regulation EU 2018/1807 refer to data portability and the aim to make it easier to port data from one IT environment to another – ie, to another provider's systems or to on-site systems. This prevents vendor lock-in and fosters competition between service providers.

However, the above Regulations differ in their approach to portability when it comes to the relation between the targeted interest groups and the legal nature of the provisions. The right to portability of personal data under Article 20 of the GDPR focuses on the relation between the data subject and the controller. It concerns the right of the data subject to receive personal data which they have provided to the controller, in a structured, commonly used and machine-readable format, and to transmit such data to another controller or to their own storage capacities without hindrance from the controller to which the personal data has been provided. Typically, the data subjects in this relation are consumers of various online services that wish to switch between these service providers.

Article 6 of Regulation EU 2018/1807 does not provide for a right for professional users to port data, but has a self-regulatory approach, with voluntary codes of conduct for the industry. At the same time, it targets a situation where a professional user has outsourced the processing of its data to a third party offering a data processing service. In accordance with Article 3 (8) of Regulation EU 2018/1807, a “professional user” can include “both natural and legal persons, including public authorities or bodies governed by public law, using or requesting a data processing service for purposes related to their trade, business, craft, profes-

sion or task”. In practice, the portability under Article 6 of the Free Flow of Non-Personal Data Regulation concerns business-to-business interactions between a professional user (which may qualify as a “controller” in accordance with the GDPR in cases that include the processing of personal data) and a service provider (similarly, to be qualified in some cases as a “processor”).

3.4 Regulators and Enforcement

The Ministry of Digital Governance is responsible for matters of data governance, such as cloud infrastructures and interoperability. The National Cybersecurity Authority is the competent body for the security of information systems and access to data. Although the Regulation on the free flow of non-personal data does not establish a new supervisory authority, its implementation often interacts with the HDPA, particularly when datasets are mixed and include both personal and non-personal data.

The Hellenic Competition Commission also plays an important role, especially in relation to the enforcement of the Digital Market Act (DMA). In Greece, the authority responsible for ensuring compliance with the DMA is the Competition Commission, particularly regarding the obligations imposed on gatekeepers, such as:

- the prohibition on combining personal data for advertising purposes unless the user consents (Article 5 (2) of the DMA);
- the prohibition on using non-public data generated or provided by the gatekeeper's business users to compete against them (Article 6 (2) of the DMA);
- the obligation to provide access to data (Article 6 (10) of the DMA); and
- the obligation to provide access to search data (Article 6 (11) of the DMA).

4. Sectoral Topics

4.1 Use of Cookies

The use of cookies is governed by Law 3471/2006 and Recommendation 1/2020 of the HDPA. The basic requirement for the use of cookies is to obtain the

prior informed consent of the subscriber or user of the terminal equipment. More specifically:

- the consent requires a clear positive act (“opt-in”) and cannot be inferred (ie, preselected cookies, inferred acceptance by scrolling); and
- consent must be given after the appropriate information of the subscriber or user, including the purpose of processing each cookie separately, the term of operation, the identity of the data controller, and the data recipients or categories of recipients.

As an exception to the above, prior informed consent is not required for cookies that are technically necessary to connect to the website or obtain the internet service requested by the subscriber or user, such as:

- cookies necessary to authenticate the subscriber or user for services that require authentication (ie, for banking transactions via the internet);
- cookies for the purpose of safety of the subscriber or user, such as cookies that detect repeated unsuccessful attempts to log in to the user’s account on a specific website;
- cookies necessary for load balancing; and
- cookies that “remember” the subscriber’s or user’s choices regarding the presentation of the website (ie, cookies related to the choice of language).

Cookies installed for the purpose of online advertising, either first-party or third-party cookies, and cookies for the purpose of statistical analysis (eg, Google Analytics) are not included in the above exceptions and require prior informed consent.

4.2 Personalised Advertising and Other Online Marketing Practices

According to law 3471/2006 for the protection of personal data in the sector of electronic communications, personalised or targeted advertising and other online marketing practices require the express consent of the data subject. Market research does not qualify as advertising to the extent that it does not conceal any commercial or other forms of advertising. Advertising communications through electronic means include:

- emails;
- messages through mobiles (SMS, MMS);

- faxes;
- instant messaging;
- electronic messaging services, such as through social networking sites; and
- calls without human intervention, such as through an automated call system.

If the data subjects have not given their prior consent, the above communications are considered unwanted (ie, “spam”), and the data subjects can file a complaint with the HDP.

Exceptionally, advertising communications through electronic means can take place without the express consent of the data subject, provided:

- the personal data has been acquired legally in the context of the sale of goods or supply of services or other transactions;
- the personal data is being used for the direct marketing and promotion of similar goods or services; and
- the data subject has been given the option to object in a clear and precise manner, easily and without cost, to the collection and use of his/her electronic personal data both at the time of collection of the data and in every message (Article 11 par 3 of Law 3471/2006).

Telephone calls with human intervention are permitted if the data subject has not objected to receiving such calls (“opt-out”) 30 days before such calls. The data subject can state his/her objection to either the data controller or the telephone service provider (mobile or fixed). All telephone service providers must keep a public record with the “opt-out” subscribers (Article 11 par 2 of Law 3471/2006, as amended by Article 16 of Law 3917/2011), accessible to anyone interested in direct advertising.

Minors can consent to the processing of their personal data if they are at least 16 years old and the data controller uses clear, accurate and simple language to inform the minors prior to obtaining their consent. When it comes to the internet and the provision of services to minors, minors can consent to the processing of their personal data if they are at least 15 years old. If minors are under this age, the consent must be

granted by their legal representative – ie, parent or legal guardian. Profiling for promotional or marketing purposes is prohibited for minors.

Advertising communications must:

- state clearly and precisely the identity of the sender;
- include instructions for the recipient to object to and stop receiving further advertising communications; and
- state their “commercial” nature in the message’s subject matter, if any.

The HDPa has issued Guideline 2/2011 with examples and best practices for obtaining the data subject’s consent electronically.

4.3 Employment Privacy Law

The organisation and management of work and the observance of the employer’s legal obligations require the processing of employees’ personal data. The provisions applicable to processing employees’ personal data (included in the GDPR and Law 4624/2019) are outlined below.

- The legal basis for the processing of the personal data of the employees is the performance of the employment contract (Article 6 par 1 (b) of the GDPR). The legal basis for the processing of special categories of employees’ personal data is the exercise of rights or the performance of legal obligations deriving from employment law, social security law and social protection law (Article 9 par 2 (a) of the GDPR).
- The legal basis of consent (Article 6 par 1 (a) of the GDPR) should be used only when there is no other legal basis for the processing of personal data of employees, taking into account the clear inequality between the data subject (employee) and the data controller (employer).
- The basic legal principles governing the processing of personal data – namely the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, and accuracy (Article 5 of the GDPR) – also apply to the processing of employees’ personal data. If any of the above principles

is breached, the processing should be considered illegal.

- The processing of employees’ personal data by means of CCTV in the workplace, whether publicly accessible or not, is permitted only if it is necessary for the protection of persons and property. Data collected through CCTV may not be used to assess employee efficiency and performance, nor to track working hours. Employees must be informed in advance in writing of the installation and operation of any CCTV system in the workplace.

The HDPa has issued many guidelines and decisions on the processing of employees’ personal data, including Guideline 115/2001 on the protection of employees’ personal data and Guidelines 1/2021 and 2/2020 on the protection of personal data in remote working (telework).

4.4 Data Protection in M&A

In business mergers and acquisitions, as well as during due diligence, where the exchange of information is necessary for the completion of the transaction, there is no specific legislation that sets out special requirements regarding the privacy and security of personal and non-personal data. On the contrary, the general legislation applies, including the GDPR and Law 4605/2016 on the protection of trade secrets, along with the provisions set by the parties in the Non-Disclosure Agreement, which usually deals with such issues. In addition, Law 3959/2011 on free competition provides for the cases that require notification of the merger to the Hellenic Competition Authority, which assesses the nature of the exchanged information as confidential.

5. International Considerations

5.1 Restrictions on International Data Transfers

The transfer of personal data from an EU member state to another EU member state may take place freely (Article 44 of the GDPR), provided the other provisions of the GDPR are met. The transfer of personal data from an EU member state to a non-EU country or international organisation may take place

freely if the European Commission decides that such a non-EU country or international organisation ensures adequate protection for personal data. Such transfer shall not require any specific authorisation (Article 45 of the GDPR).

In the absence of such an adequacy decision by the European Commission, transfers of personal data to a non-EU country or international organisation may take place subject to appropriate safeguards provided by the data controller or data processor and on the condition that enforceable data subject rights and effective legal remedies are available. Such transfer shall not require any specific authorisation (Article 46 of the GDPR).

Appropriate safeguards may be provided by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;
- standard data protection clauses adopted by the European Commission;
- an approved code of conduct; or
- an approved certification mechanism.

In the absence of an adequacy decision and appropriate safeguards, transfers of personal data to a non-EU country or international organisation may take place only on one of the following conditions (Article 49 of the GDPR):

- the data subject has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfer for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the data controller, or for the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;

- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or of other persons where the data subject is physically or legally incapable of giving consent; or
- the transfer is made from a register which, according to EU or member state law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or member state law for consultation are fulfilled in the particular case.

For non-personal data, Article 4 of Regulation (EU) 2018/1807 states that free flow is the rule, and data localisation is the exception, if justified on grounds of public security in accordance with the principle of proportionality.

The GDPR does not provide a legal definition of the concept of “transfer of personal data to a third country or an international organisation”. In EDPB Guidelines 5/2021, three cumulative criteria are set out that must be met in order for a processing operation to be characterised as a “transfer”:

- the controller or processor (“exporter”) is subject to the GDPR with regard to the specific processing;
- the exporter discloses by transmission or otherwise makes available personal data that is subject to that processing to another controller, joint controller or processor (“importer”); and
- the importer is located in a third country, regardless of whether the importer is subject to the GDPR for the given processing under Article 3, or is an international organisation.

Furthermore, according to EDPB Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, remote access by an entity in a third country to data located in the EEA is also considered a transfer. Therefore, provided that the above criteria are met, remote access is regarded as a transfer.

5.2 Government Notifications and Approvals

In Greece, no authorisation is required for the international transfer of data, meaning that no specific registrations, notifications or approvals from national authorities are necessary for such transfers. Please see **5.1 Restrictions on International Data Transfers** regarding international transfers of personal data.

However, the data controller or processor must enter the transfers of personal data in the records of processing activities (Article 30 of the GDPR), stating at least the recipient and the documentation proving the existence of appropriate safeguards. Such records, including records of transfers, should be made available to the HDPa upon request.

5.3 Data Localisation Requirements

In general, Regulation (EU) 2018/1807 promotes the free flow of non-personal data across EU member states. EU member states can only impose localisation requirements for non-personal data if doing so is justified on grounds of public security, in compliance with the principle of proportionality.

In the above context, there are laws that require the localisation of non-personal data in sectors such as:

- taxation and social security;
- customs; cybersecurity; and
- specific sectors of the government regarding the Ministry of National Defence, the Ministry of Citizen Protection, the Ministry of Foreign Affairs, the Coast Guard of the Ministry of Shipping, the General Secretariat of Citizenship of the Ministry of Interior, the National Intelligence Service and the services of Criminal Records of the Ministry of Justice.

Please see **5.1 Restrictions on International Data Transfers** regarding whether or not remote access to data is considered a transfer.

5.4 Blocking Statutes

There are no “blocking” statutes in Greece, meaning there are no Greek laws or statutes that prohibit compliance with EU regulations. Every international transfer of personal and non-personal data must comply with EU transfer rules. Requests for data transfers originating from third countries cannot be fulfilled unless they are consistent with these rules. Article 48 of the GDPR provides that any judgment of a court or decision of an administrative authority of a third country requiring a data controller or processor to transfer or disclose personal data may be recognised or enforced in any way only if it is based on an international agreement, such as a mutual legal assistance treaty, that is in force between the requesting third country and the EU or a member state, without prejudice to other grounds for transfer.

5.5 Recent Developments

Greece is steadily investing in improving data governance, data protection and cybersecurity, and in upgrading its digital infrastructure. These initiatives align with the EU’s digital decade objectives and help to create the conditions for future developments and legal frameworks. As Greece’s digital maturity continues to grow, it is likely that new measures or further clarifications in the area of data international transfers will emerge in the coming years.

INDIA



Trends and Developments

Contributed by:

Sandra Lisa Philip, Shri Gayathri and Prashanth Shivadass
Shivadass & Shivadass

Shivadass & Shivadass is a boutique law firm headquartered in Bangalore, India that focuses on taxation, competition law, intellectual property and data protection – from a consultative and compliance outlook and an adversarial spectrum. The firm’s highly regarded disputes practice aids and represents clients across multiple fora, specifically in taxation and competition law (with one of its partners also being the panel counsel for the Competition Commission of India), making the firm one of the most sought-

after firms in the market. The firm’s data privacy and protection practice stems from its team of seven member’s inherent understanding of technological advancements and opportunities in India. It advises multinational corporations, Indian entities and Indian start-ups on compliance best practices, including consent management, structuring privacy and cookie policies, cross-border data transfers, data minimisation and retention, breach strategies and general agreements with third-party data processors.

Authors



Sandra Lisa Philip is a lawyer who specialises in data protection and commercial litigation, with experience in advising clients on regulatory compliance, privacy frameworks and complex commercial disputes. Her

practice focuses on navigating data protection laws, risk management, contractual enforcement, and dispute resolution across diverse business sectors. Her professional contributions include authoring legal insights on topics relating to data protection, privacy law, commercial litigation and regulatory developments. She regularly engages in legal research and analysis, translating complex legal issues into clear, insightful commentary for professionals and businesses.



Shri Gayathri is an advocate at Shivadass & Shivadass, practising in areas that include data protection, privacy law and indirect tax litigation. She contributes to the firm’s legal advisory and compliance work,

supporting clients with regulatory guidance, risk mitigation and dispute resolution strategies. Her professional contributions include co-authoring legal insights and guides on data protection compliance and competition law topics for industry platforms and legal publications.



Prashanth Shivadass is an advocate and partner at Shivadass & Shivadass. He holds a post-graduate degree in Competition Law from Queen Mary University of London.

Prashanth advises both domestic and international clients on a variety of areas, including taxation, competition and antitrust laws, data protection and allied laws, company and corporate laws, across various sectors. Prashanth has also appeared in over 1,000 commercial litigation, corporate, taxation (direct and indirect) and competition matters for clients all over India, including before various Tribunals, High Courts and the Supreme Court. Prashanth is also an empanelled advocate for the Competition Commission of India (CCI), representing the CCI across different fora (effective 2024).

Shivadass and Shivadass

4/2 Millers Road
Level 3
Bangalore 560052
India

Tel: +91 80 4377 9955
Email: admin@sdlaw.co.in
Web: www.sdlaw.co.in



AI and Privacy: What Is Next for India?

Introduction

India is widely regarded as being in its “techade”, where technology is expected to drive economic growth and business efficiency. Artificial intelligence (AI) is already playing a central role in this shift. Indian businesses are no longer testing AI at margins but are actively using it across core operations to improve productivity, manage risk and scale faster. Industry reports (eg, *Nasscom AI Index Adoption*) show that a significant number of Indian enterprises now have AI tools deployed in sectors such as banking, healthcare, retail, manufacturing and technology services. The adoption of AI poses a threat to human employment.

For businesses, the attraction of AI lies in its ability to process large volumes of data quickly and turn it into useful actionables. AI is used to detect fraud, predict demand, personalise customer interactions, automate internal processes and support management decisions that would otherwise require substantial time and human effort. In consumer-facing sectors, AI powers user algorithms, shopping indices, targeted advertising and recommendation engines, which influence what customers see, buy and engage with.

This rapid adoption of AI has made data a critical business asset. Most AI systems depend on continuous access to data, including customer information behavioural patterns and, sometimes, sensitive personal details. As a result, questions around how data is collected, used and safeguarded are no longer a purely legal issue but are also a concern for boardrooms, since they directly affect trust and brand value.

As AI becomes central to business growth and efficiency, organisations must focus not only on what AI can do but also on how it is used. This requires clear internal oversight, thoughtful data practices and an awareness of various privacy risks that arise from large-scale data use. Going forward, businesses that balance innovation with care and responsibility will be better suited to grow, build customer trust and stand out in the market. In the long run, trust and responsible AI use will be key to becoming a leader in the AI market.

AI Adoption Across Key Business Sectors in India

Banking and financial

AI is a widely used technology in the banking and financial services sector – statistics indicate that close to two thirds of banks and financial institutions operating within India have already integrated AI into their operations (*Nasscom AI Index Adoption*).

Banks have been developing their own “generative AI”; initially, its usage was restricted to customer services. Various chatbots have now been incorporated for rendering customer services and to provide financial advice. Some banks also use AI robot tools and voice recognition tools to perform compliance checks, data entry, know-your-customer (KYC) verification, email responses and other customer support services.

AI is also now being widely used in fraud detection to detect unusual patterns in banking, such as rapid micro-transactions or logins from suspicious devices. The Reserve Bank of India recently also launched the Digital Payments Intelligence Platform (DPIP), which harnesses AI to detect fraudulent transactions and

prevent payments across UPIs. Banks and non-banking financial companies (NBFCs) use AI tools such as Feedzai and Verafin (available in the public domain) to secure payments and stop fraudulent transactions, and for identity verification, scam prevention, account monitoring, malware detection, phishing, etc. These systems help reduce manual oversight, speed up decision-making and improve the accuracy of risk assessments.

Healthcare and Pharmaceuticals

Hospitals and healthcare systems in India are using AI to support diagnostic imaging, clinical decision support, predictive patient risk profiling, personalised treatment recommendations and administrative automation. Leading healthcare networks are deploying AI tools such as Dax Copilot and Storyline AI (available in the public domain) to transcribe clinical notes, generate discharge summaries, support telemedicine and assist with diagnostic workflows, helping address rising patient volumes.

AI has emerged as one of the most powerful tools in the pharmaceutical industry as well. Generative AI such as AlphaFold2 (AF2) and NovaFold AI (available in the public domain) are used for molecular design, drug design, etc. This allows for identifying potential drug targets more efficiently, which helps prioritise compounds for experimental testing. Beyond discovery, AI also predicts patient eligibility and helps with strategising dosage to identify safer candidates for such experimental testing, eradicating extensive animal testing as a whole.

Manufacturing

Manufacturing and industrial sectors are increasingly adopting AI to improve operations and reduce downtime. AI-enabled systems support predictive maintenance of equipment and quality control through automated defect detection and optimisation of production schedules. AI is also at the heart of robotics and automation. A widely known example is Tesla's Optimus humanoid robot, which has been developed to carry out tasks such as lifting, assembly or anything that may otherwise be dangerous for humans. While AI adoption in manufacturing currently trails behind banking and healthcare, it is increasing as companies

see the benefits of AI in reducing waste and enhancing supply chains.

Retail

Consumer goods and retail businesses are using AI for consumer insights, personalised marketing, etc. Retailers use algorithms to analyse large volumes of sales and consumer data, tailoring promotions for different customer segments. Similarly, consumer goods companies are embedding AI into product development to respond swiftly to changes in consumer preferences.

Marketing

AI in marketing is not optional – it is a power source. Smart data analytics, targeted campaigns, content creation, ad creation, data analysis, research and behavioural analysis of customers is impossible in “techade” without AI. Various AI tools have been deployed to execute strategies within minutes instead of weeks.

Technology and Telecommunication

AI plays a crucial role in enhancing efficiency, reliability and customer experience. Telecommunication companies use AI to optimise network performance wherein they predict traffic patterns, managing bandwidth and detecting faults, thereby preventing service disruptions. On the customer side, AI powers chatbots and virtual assistants, handles service queries, troubleshoots issues and personalises plans based on usage patterns.

Facial recognition technology uses computer vision and machine-learning algorithms to identify or verify individuals based on their facial features. By analysing patterns including distance between eyes, facial contours and unique facial landmarks, AI tools can accurately match faces against stored databases. This is also being used in areas such as smartphone authentication, surveillance and security, access control and digital payments. In workspaces, facial recognition is being used for access control in devices for authentication, in retail environments for customer analytics, and in digital services for onboarding and verification.

Apart from the above, generative AI is specifically used across businesses for reviewing documents,

extracting key information, summarising documents, drafting and interpreting legal clauses, obtaining a nuanced understanding of language and context, applying business logic, sending automated emails, linking information, etc.

While the adoption of AI across key business sectors offers significant potential for advancement, it is also accompanied by a number of drawbacks.

High-Risk AI Applications in Business Practices

AI-related privacy risks can be understood better when examined through real-world business use cases. Certain AI applications warrant closer scrutiny as they are both widely used by businesses and inherently high-risk from a privacy perspective. These risks can be divided between:

- technological risks; and
- sectoral risks by the use of AI.

Technological risks

Generative AI

Generative AI possesses significant privacy risks across business sectors, as it relies on vast datasets that may contain sensitive or personal information. This increases the risk of data leakage or unintended disclosure through generated outputs.

In business environments, generative AI can inadvertently reproduce confidential data, trade secrets or personally identifiable information if the training module is not properly governed. Prompts pertaining to proprietary or customer data given by employees in order to obtain business ideas/logic may continue to be reflected in the chat history of other users, thereby exposing confidential information. Additionally, limited transparency around how generative AI models store, learn from and retain data makes privacy compliance more complex.

Facial recognition technology

Businesses that adopt facial recognition – ie, because it reduces friction, lowers dependency on passwords and enables rapid identification at scale – face privacy risks with the nature of data itself. Facial data is deeply personal, permanently linked to an individual and can-

not be replaced if compromised. Once collected, misuse or leakage can carry long-term consequences.

Most privacy issues in facial recognition arise from unclear purpose definition and over-collection of data. Risks are significantly reduced when organisations clearly specify where and why facial data is used, restrict its application to narrowly defined functions and avoid repurposing it across unrelated systems. Meaningful opt-in mechanisms, rather than default or passive consent, are critical.

From a technical standpoint, privacy risks can be reduced by converting facial images into encrypted biometric templates, keeping the data only for as long as necessary and avoiding centralised storage. Regular testing for accuracy and bias is equally important. However, most reliance is placed on internal policies. These should clearly define acceptable and prohibited users and prevent the gradual expansion of facial recognition into areas where it was never intended.

Sectoral risks by the use of AI

Lending and banking operations

Banks and NBFCs' reliance on AI, if effected without precautions, can have long-term disastrous consequences for customers, since it deals with some of their most sensitive data and even a slight overlook can put them in the way of cyberthreats. AI's help in accelerating banking decisions and credits is a huge attraction for these institutions as well as their customers.

Most privacy issues in this sector emanate from similar concerns surrounding hoarding and use of data, especially with credit and banking details. Use of these datasets after the purpose of retention, if used to train AI models, can either result in bias or the worse consequences of such data falling into the wrong hands. Data minimisation and purpose limitation – the two core principles of data privacy – must be applied here too, to ensure that such risks are nipped in the bud.

Healthcare and pharmaceuticals

AI tools used in the healthcare sector for processing data/information pertaining to patients rely on highly sensitive data and directly affect individuals. As already discussed, the benefits of AI in the healthcare

sector are not negligible. Contributions this massive also come with their own risks such as data breaches, algorithm bias, and regarding understanding consent and the extent of its application. Data anonymity can be a starting step to train AI models, ensuring that its learning is not influenced by failing to feed it enough data but, at the same time, that raw patient data is not put at risk.

Since most consumers are unaware of the extent to which their data is used, it is imperative that such extent be clearly delineated and explained to them so that they are in a position to give informed consent, and that businesses do not lack accountability when questioned.

The AI-Privacy Gap in Business Operations

The AI-privacy gap in business operations does not arise because organisations are unaware of privacy risks but because AI systems fundamentally change how data is collected, combined and reused within organisations. Unlike traditional IT systems, AI models are rarely limited to a single dataset or a single purpose. Businesses routinely feed AI systems with data drawn from consumer interactions, transaction histories, third-party datasets and publicly available information to improve accuracy and performance. Over time, this creates complex data chains that are difficult to map, monitor and control.

One of the most significant gaps appears at the point of data aggregation. Businesses often collect data for a refined operational purpose such as customer onboarding, service delivery or compliance, but later reuse the same data to train or fine-tune AI models for analytics, personalisation or prediction. While this may make commercial sense, it creates uncertainty around whether individuals are aware of, or expect, such secondary uses.

A close second issue is the use of third-party and cloud-based AI tools. Many Indian businesses rely on external platforms for generative AI, analytics, facial recognition or customer engagement. While these tools offer speed and scalability, they often operate as “black boxes”. Businesses may have limited visibility into how prompts, inputs or datasets are stored, whether they are retained for model improvement, or

how long they stay across systems. This lack of transparency increases the risk of unintended data exposure, especially when sensitive personal or commercial information is used in routine business workflows.

The AI-privacy gap is further widened by the dynamic nature of AI systems. Unlike static software, AI models evolve as they are trained on new data or adapted data, for new use cases. Insights generated by AI, such as behavioural predictions or risk scores, may go beyond the data that was originally collected. In many cases, even development teams may not fully anticipate the types of inferences that AI systems can generate once deployed at scale. This creates challenges for businesses trying to align AI outputs with governance standards.

Importantly, this gap is not unique to India but is amplified by the speed of adoption. Industry reports (Deloitte Asia Pacific survey) consistently show that Indian businesses are among the fastest adopters of AI and generative AI globally, often outpacing the maturity of internal governance frameworks. In many cases, business value is realised faster than risk controls can be put in place. As a result, governance mechanisms tend to mature only after systems are already in use, increasing exposure to privacy and reputational risks.

In India, this AI-privacy gap is in part shaped by the Digital Personal Data Protection Act, 2023 (DPDPA), which operates as an indirect but influential constraint on how businesses deploy AI. While the DPDPA does not regulate AI systems as such, it governs how personal data used by organisations – including data processed through AI tools – is collected, processed, stored and shared. In practice, this means that businesses remain responsible for the downstream effects of AI-driven data processing, regardless of whether AI systems are developed internally or sourced from third-party vendors.

Alongside the DPDPA, India’s emerging AI governance approach relies heavily on policy principles rather than binding rules. The “India AI Governance” framework emphasises responsible use, transparency, fairness, safety and human oversight, signalling how regulators and courts are likely to evaluate AI deployment

in the future. For businesses, this creates a mixed landscape. On one hand, companies have the freedom to design AI governance frameworks that align with their specific use cases and risk profiles. On the other hand, the absence of clarity makes it difficult to assess long-term compliance exposure. Businesses must therefore operate with the understanding that today's voluntary guidelines may form the basis of tomorrow's regulatory benchmarks.

Managing AI Risks in an Interim Governance Landscape

The absence of a concrete AI regulation shifts the onus onto organisations for navigating an interim governance landscape where risk management must be driven internally. For many businesses, this has shifted the focus from formal compliance to internal operational structures. AI systems are increasingly embedded across customer-facing functions, internal decision-making and core commercial processes, making it essential to evaluate not just whether AI is used but also how it is used and monitored over time.

Contractual and technical safeguards play a critical role here. Businesses must ensure that agreements with technology providers and service vendors address data protection responsibilities, security standards and limitations on data reuse.

As already mentioned, internal policies also play a central role in this phase. Businesses are increasingly expected to articulate their own standards for responsible AI use. Clear internal guidance on acceptable applications, human oversight and escalation mechanisms helps to ensure that AI systems support business objectives without creating unmanaged privacy or ethical risks. These measures allow organisations to operate responsibly while remaining adaptable to future legal developments in AI.

Corporate AI Guidelines

Given that Indian businesses are increasingly relying on generative AI across functions such as content creation, analytics, customer engagement and internal productivity, the privacy and governance risks associated with these systems have become particularly pronounced. Generative AI is associated with risks such as violations of the user's privacy, concerns

about infringement of the user's rights, loss of trade secrets and breach of privacy clauses.

It is therefore imperative that every company come up with an AI policy internally. This policy must clearly delineate permitted uses of AI and expressly prohibit impermissible applications. Informed and responsible use of AI must be encouraged in order to increase efficiency, innovation, etc, and the risks associated with AI should be explained in the policy. A list of approved AI tools must be circulated and a formal process for approving additional tools must be established. The privacy policy for AI tools is to be thoroughly produced before approving the usage of such tools. The policy should:

- specify whether and to what extent user conversations may be used to train or improve AI models;
- clarify that prompts should not be shared with non-service providers or third parties without the consent of the user;
- clarify whether user prompts can be shared with its service providers, law enforcement agencies, research partners, third parties and affiliates;
- lay down the level of transparency and accessibility of information regarding how AI models are trained;
- identify the categories and sources of data used to train AI models; and
- address whether and how users' personal information can be removed or excluded from training datasets.

Most privacy risks are best managed through deliberate design choices. Wherever possible, organisations can limit exposure by removing direct identifiers, using anonymised or pseudonymised datasets and adopting training methods that do not require raw data to leave secure environments. Clear communication with users about how their data is used, combined with consent processes that are genuinely understandable rather than buried in documentation, plays a critical role in building trust. These measures must be reinforced through strong internal governance such as the policy guideline itself, routine audits of AI systems and strict controls on data sharing, particularly when working with external technology vendors.

Conclusion

Fundamentally, applying India's existing legal framework to AI-driven business activity requires documentation and adaptability. Businesses that proactively embed privacy and AI governance into their operational culture are better positioned to respond to regulatory change. Companies must proactively interpret privacy obligations, embed AI governance into internal decision-making and adopt self-regulatory practices that address risks not yet fully captured by law.

The risks associated with AI do not arise from its use alone but from the absence of clear internal boundaries around how data is collected, processed, shared and retained. The most effective risk management strategies, therefore, lie in shaping how it is designed and governed within organisations.

A recurring lesson across AI risk management practices is that less invasive systems are often the most sustainable. Transparency in how AI tools function, restraint in data collection, meaningful consent and clear opt-out mechanisms consistently reduce privacy concerns. Techniques such as anonymisation, restricted data retention, decentralised training models and limited reuse of data will allow organisations to retain the benefits of AI while considerably reducing the chances of misuse and leaks.

However, it is also important to acknowledge the trade-off between data minimisation and performance. In many cases, AI systems that rely on richer and more diverse datasets can deliver more accurate and reliable results. Expecting high-quality results from severely data-restricted systems is often unrealistic. The real challenge, therefore, is not to eliminate data use but to be deliberate about it. Organisations must focus on collecting data that is only relevant to the task at hand.

Equally important is the role of organisational AI policies. Without clearly articulated internal rules, AI systems tend to expand beyond their original purpose, incorporate new datasets and be used in ways that were never intended. Corporate AI guidelines that define permitted use cases, restrict high-risk applications, vet third-party tools and set minimum transparency standards act as practical safeguards.

Ultimately, reducing AI-related privacy risks is less about reactive controls and more about organisational discipline. Until clearer and more comprehensive regulation comes into the picture, the balance between innovation and self-regulation will remain central to how businesses responsibly leverage AI.

INDONESIA



Law and Practice

Contributed by:

Raditya Kosasih, Dimas Triandhanu Utomo, Nicholas Glenn and Nabila Oktavia Annyndira
ALTA Advocates

Contents

1. Legal and Regulatory Framework p.158

- 1.1 Overview of Data and Privacy-Related Laws p.158
- 1.2 Rights and Obligations p.159
- 1.3 Special Categories of Personal Data p.160
- 1.4 Processing of Personal Data for Research and Development Purposes p.161
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.161
- 1.6 Data Breach Requirement p.162
- 1.7 Regulators p.162
- 1.8 Enforcement Proceedings and Fines p.164
- 1.9 Enforcement Trends p.164

2. Privacy Litigation p.165

- 2.1 Privacy Litigation Overview p.165
- 2.2 Recent Case Law p.165
- 2.3 Collective Redress Mechanisms p.165

3. Requirements for the Protection and Processing of Non-Personal Data p.165

- 3.1 Objectives and Scope of Data Regulation p.165
- 3.2 Interaction of Data Regulation and Data Protection p.166
- 3.3 Rights and Obligations Under Applicable Data Regulation p.166
- 3.4 Regulators and Enforcement p.166

4. Sectoral Topics p.167

- 4.1 Use of Cookies p.167
- 4.2 Personalised Advertising and Other Online Marketing Practices p.167
- 4.3 Employment Privacy Law p.167
- 4.4 Data Protection in M&A p.167

5. International Considerations p.168

- 5.1 Restrictions on International Data Transfers p.168
- 5.2 Government Notifications and Approvals p.168
- 5.3 Data Localisation Requirements p.169
- 5.4 Blocking Statutes p.169
- 5.5 Recent Developments p.169

ALTA Advocates is an Indonesian law firm offering a comprehensive range of corporate, commercial, and technology-focused legal services. The firm advises on matters involving general corporate, mergers and acquisitions, investment, capital markets, banking and finance, debt restructuring, start-ups and venture capital, privacy and data protection, cybersecurity, artificial intelligence (AI), web3, TMT, ESG, fintech, crypto-asset trading and exchanges, and intellectual property. ALTA Advocates is well known for its strong focus on privacy and personal data protection. The

team delivers comprehensive and end-to-end services to various Indonesian and global companies to ensure their privacy and data protection compliance, including drafting internal policies, key documentation (RoPA/DPIA/privacy notices), data-sharing agreements, DPO support, trainings, and incident handling. With its deep expertise in data protection, ALTA Advocates has worked closely with stakeholders across key industries and has been actively involved in policy-making initiatives with the Indonesian government.

Authors



Raditya Kosasih is a highly experienced data protection lawyer and former Group DPO with 15+ years in both private practice and in-house roles. His practice focuses on privacy and personal data

protection, cybersecurity, intellectual property, artificial intelligence, fintech, investment, capital market, and general corporate matters. Kosasih is a co-founder of the Indonesian Association of Data Protection Practitioners (APPD), and is also a member of the International Association of Privacy Professionals (IAPP), and the OECD's Expert Community on Data Free Flow with Trust (DFFT). Kosasih is also a certified assessor for a DPO certification body in Indonesia.



Dimas Triandhanu Utomo has over 15 years of experience as a corporate lawyer, including serving as a partner at a reputable law firm and as vice president of the Legal Team at Gojek Group. His practice focuses on

general corporate and M&A matters, including fundraising, venture capital and private equity investments, start-up growth, restructuring, foreign investment, joint ventures, and corporate governance, as well as privacy and data protection. He is a member of the Indonesian Association of Data Protection Practitioners (APPD), and the International Association of Privacy Professionals (IAPP), and has passed the CIPP/E certification.



Nicholas Glenn specialises in personal data protection, and general corporate law (including corporate M&A and capital markets). His experience extends to the critical areas of end-to-end personal data

protection programme implementation, including navigating data breach incidents for clients. Nicholas has also assisted start-ups and tech-based companies in trade (retail and distribution), financial technology, telecommunications, and FMCG industries with company restructuring, fundraising legal instruments, TMT matters, and business licensing. Nicholas is a member of the Indonesian Association of Data Protection Practitioners (APPD).



Nabila Oktavia Annyndira specialises in general corporate, M&A, and personal data protection, including M&A transactions, start-up fundraising, corporate establishment and restructuring, day-to-day legal

support through retainer services, legal due diligence, and matters relating to competition and employment law. Via has been actively involved in end-to-end personal data protection services, ranging from drafting internal policies, privacy notices, RoPA and DPIA drafting and advisory, and supporting clients in the day-to-day implementation of personal data protection matters under retainer arrangements. She has worked with clients and counterparties across various key sectors. Via is a member of the Indonesian Association of Data Protection Practitioners (APPD).

ALTA Advocates

Sampoerna Strategic Square
South Tower
Level 16
Jl. Jenderal Sudirman Kav. 45-46
Jakarta 12930
Indonesia

Tel: +62-811-978-2024
Email: office@altaadvocates.com
Web: www.altaadvocates.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Law No 27 of 2022 on Personal Data Protection (the “PDP Law”) constitutes the primary legal framework for privacy and personal data protection in Indonesia. The PDP Law is enacted as an implementation of the constitutional right to privacy (as elaborated in its General Elucidation) pursuant to Article 28G(1) of the 1945 Constitution of the Republic of Indonesia.

In Indonesia, personal data is defined as data regarding individuals (referred to as data subjects) who are identified or can be identified separately or in combination with other information, either directly or indirectly, through an electronic or non-electronic system.

Personal data is classified into two categories:

- general personal data: name, gender, nationality, religion, marital status, and/or personal data that is combined to identify an individual; and
- specific personal data: health data and information, biometric data, genetic data, criminal records, children’s data, personal financial data, and/or other data as stipulated under applicable laws and regulations.

The PDP Law establishes key principles and lawful bases for personal data processing, personal data categorisation, the processing requirements for children and persons with disabilities, data subjects rights, the scope of personal data processing, and role-based compliance obligations (ie, personal data controllers,

personal data processors, and joint controllers). In addition, the PDP Law regulates the appointment of a Data Protection Officer (DPO), requirements for personal data transfer (both domestically and cross borders), administrative sanctions for non-compliance, and criminal sanctions in the event of violation. The PDP Law also addresses international co-operation in the field of personal data protection, public participation, and mechanisms for dispute resolution.

The PDP Law is expected to be supplemented by implementing regulations in the form of a government regulation. While the PDP Law governs the general framework of personal data protection in Indonesia, it is also subject to other existing and sector-specific laws and regulations. These include, among others:

- regulations in the electronic systems ecosystem:
 - (a) Law No 11 of 2008 on Electronic Information and Transactions, as lastly amended by Law No 1 of 2024 (“EIT Law”);
 - (b) Government Regulation No 71 of 2019 on the Operation of Electronic Systems and Transactions (“GR 71/2019”);
 - (c) Ministry of Communication and Digital (MOCD) No 20 of 2016 on Personal Data Protection in Electronic Systems (“MOCD Reg 20/2016”); and
 - (d) Government Regulation No 17 of 2025 on the Governance of Electronic Systems for Child Protection (“PP TUNAS”),
- other sector-specific regulations, for example, in highly regulated industries such as financial services and fintech sectors:

- (a) Financial Services Authority (*Otoritas Jasa Keuangan*, OJK) Regulation No 22 of 2023 on Consumer and Public Protection in the Financial Services Sector; and
- (b) Bank Indonesia (BI) Regulation No 3 of 2023 on BI Consumer Protection,

These sectoral regulations supplement or specify personal data protection rules, provided they do not conflict with the PDP Law.

The PDP Law has extraterritorial reach, applying to individuals or corporations, public bodies, or international organisations that conduct legal acts as regulated under the PDP Law, whether:

- within the territory of the Republic of Indonesia; or
- outside Indonesia where such acts have legal effects in Indonesia and/or to Indonesian citizens as personal data subjects abroad.

The PDP Law does not apply to the processing of personal data by individuals for purely personal or household purposes.

1.2 Rights and Obligations

General Principles of Personal Data Processing

In Indonesia, the processing of personal data encompasses the entire life cycle of personal data, from collection, analysis, storage, rectification, display, announcement, transfer, disclosure, deletion, and destruction of personal data. Such personal data processing must follow these principles:

- **Lawful, Fair, and Transparent:** Processing shall be processed based on a lawful basis provided under the PDP Law. Processing shall be carried out fairly, transparently, and in a limited and specific manner, in line with the purposes communicated to the data subject. Personal data controllers are required to provide clear and accessible information to data subjects regarding the personal data processing practices.
- **Data Minimisation:** Personal data processing shall be relevant and limited to what is necessary for the intended purposes.

- **Purpose Limitation:** Personal data shall be processed only for specified purposes that are clearly communicated to data subjects.
- **Data Subject Rights:** The rights of data subjects shall be respected and supported through appropriate processes.
- **Accuracy and Completeness:** Personal data shall be accurate, complete, and kept up-to-date.
- **Accountability:** Processing shall be carried out responsibly and in a demonstrable manner, supported by appropriate documentation, and supervised through periodic audits to ensure ongoing compliance with applicable laws.
- **Security and Confidentiality:** Personal data shall be processed with appropriate technical and organisational safeguards to ensure security, integrity, confidentiality, and protection against any misuse, loss, and unauthorised access, disclosure, alteration, or destruction of personal data.
- **Retention, Deletion (*Penghapusan*), and Destruction (*Pemusnahan*):** Personal data shall be retained only for as long as necessary for lawful processing purposes, in accordance with the retention schedule and the applicable laws.

Data Subject Rights

Under the PDP Law, the data subjects' rights are recognised, including:

- (i) the right to obtain clear and transparent information regarding the personal data controller, lawful basis for processing, purpose of the collection and use of personal data, and the accountability of the party requesting such personal data;
- (ii) the right to file a claim and receive compensation for any violation of personal data processing relating to the data subject;
- (iii) the right to obtain and/or use personal data relating to the data subject from the personal data controller in a structured format commonly used and/or readable by electronic systems;
- (iv) the right to complete, update, and/or correct errors or inaccuracies in personal data relating to the data subject;
- (v) the right to access and obtain a copy of personal data relating to the data subject;
- (vi) the right to withdraw previously granted consent for the processing of personal data relating to

- the data subject;
- (vii) the right to proportionally restrict the processing of personal data relating to the data subject in certain circumstances;
- (viii) the right to request the termination of processing, the deletion and/or destruction of personal data relating to the data subject; and
- (ix) the right to object to the processing of personal data based on an automated decision-making process, including profiling, which has a significant impact to the data subject.

The PDP Law further provides a response mechanism for the exercise of data subject rights. Where a personal data controller receives a request for the exercise of the rights referred to in items (iv) to (vii) above, the controller is required to fulfil such request within 3 x 24 hours (ie, within 72 hours).

Role-Based Compliance Obligations under the PDP Law

The main compliance of each organisation depends on its role. The PDP Law recognises several distinct roles, each subject to specific responsibilities, liabilities, and regulatory obligations, namely the personal data controller, personal data processor, and joint controller.

- **Personal Data Controller:** As the party that determines the purposes of personal data processing and generally exercises control and responsibility, its key obligations include:
 - (a) ensuring that personal data is processed lawfully in accordance with the applicable lawful basis under the PDP Law;
 - (b) establishing and implementing a governance and compliance framework, including appropriate data governance structures, internal policies, and procedures, as well as continuously monitoring compliance;
 - (c) providing privacy notices and ensuring transparency to data subjects;
 - (d) classifying and handling personal data appropriately, including applying the required safeguards for each category of data (general and specific personal data);
 - (e) implementing adequate security and confidentiality measures;

- (f) ensuring the accuracy and integrity of personal data through verification and update mechanisms;
 - (g) conducting a data protection impact assessment (DPIA) in the event that the processing of personal data has the potential to pose a high risk to the data subject;
 - (h) establishing and maintaining records of processing activities (RoPA);
 - (i) ensuring that data transfers and third-party engagements comply with the PDP Law;
 - (j) implementing incident or personal data breach handling procedures, including notification within 3 x 24 hours (ie, within 72 hours);
 - (k) establishing a data retention schedule and mechanism for deletion and/or destruction in accordance with applicable laws;
 - (l) appointing a DPO, where required; and
 - (m) handling data subject rights.
- **Personal Data Processor:** A personal data processor is required to process personal data strictly based on the instructions of the personal data controller and must obtain the controller's prior written approval if it engages another personal data processor (sub-processor). Primary liability for personal data processing rests with the personal data controller. However, a personal data processor may be held independently liable where it processes personal data contrary to the controller's instructions, or where it violates applicable laws and regulations.
 - **Joint Controller:** Joint controllers are also required to comply with all obligations applicable to personal data controllers. Two key obligations must be observed:
 - (a) The controllers are required to enter into an agreement that sets out the roles, responsibilities, and legal relationship between the parties.
 - (b) Joint personal data controllers are jointly responsible for providing information to data subjects, including the controllers involved, lawful basis, purpose, category of personal data, methods and contact person.

1.3 Special Categories of Personal Data

The PDP Law does not set out separate processing regimes for general personal data and specific personal data. However, the processing of specific per-

sonal data may trigger additional regulatory obligations. Under PDP Law, such processing may: (i) serve as an indicator of “high-risk processing”, thereby requiring the conduct of a DPIA or risk assessment; or (ii) serve as one of the indicators for the mandatory appointment of a DPO.

Processing of Children and Persons with Disabilities

The PDP Law further provides that the processing of children’s personal data and the personal data of persons with disabilities must be carried out in a specific manner and subject to additional requirements. In the case of children, processing requires parental consent and/or legal guardians in accordance with applicable laws and regulations. For persons with disabilities, processing must be conducted using appropriate communication methods as regulated under applicable laws, and requires consent from the individual concerned and/or their legal guardian.

In addition, the processing of children’s (defined as individuals who use or access the products, services, and features and are under 18 years of age) personal data through electronic systems is subject to PP TUNAS (see **1.1 Overview of Data and Privacy-Related Laws**). PP TUNAS applies to all electronic system operators (ESOs), both public and private, whose products, services, or features are intended for use by children or are likely to be accessed by them. As an implementing regulation of the EIT Law, PP TUNAS introduces a range of obligations and prohibitions relating to children’s privacy and personal data protection, including requirements on parental consent and notification, high-privacy settings by default, the conduct of DPIAs, and the appointment of a DPO, as well as prohibitions on profiling and precise geolocation tracking by default, and manipulative practices (any methods, techniques, or non-transparent practices that can encourage children to overshare data, disable privacy settings, or engage in harmful behaviour), are strictly forbidden.

1.4 Processing of Personal Data for Research and Development Purposes

In principle, the PDP Law does not prohibit the processing of personal data or anonymise data for research and development purposes, provided that

such processing complies with the PDP Law and any applicable sector-specific regulations (for example, healthcare regulations).

Although the PDP Law does not currently contain specific provisions governing research and development activities, it recognises that certain data subject rights may be exempted for public interest purposes, including for statistical purposes and scientific research.

Where personal data is processed for the statistical activities and scientific research, the exempted rights are (i) the right to withdraw consent; (ii) the right to object to automated decision-making and profiling; (iii) the right to restrict processing; (iv) the right to data portability; and (v) the right to request the termination of processing, deletion, and/or destruction of personal data.

Accordingly, while the PDP Law does not provide a dedicated research and development regime, it allows limited restrictions on certain data subject rights, without relieving compliance with the core principles and obligations under the PDP Law.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Indonesia’s legal framework on artificial intelligence (AI) is still in an emerging stage, and there is currently no comprehensive statute governing the development or use of AI. Regulatory oversight is fragmented and primarily derived from existing, sector-specific laws and policy instruments issued and supervised by various authorities. These include, among others, the MOCD, which issued Circular Letter No 9 of 2023 on AI Ethics, as well as sectoral guidance from other regulators, such as the OJK, which introduced the OJK and Fintech Associations AI Code of Ethics. The personal data protection-related aspects under these instruments are relatively general in nature. They require that any processing of personal data involving automated decision-making and AI systems comply with the PDP Law and other applicable regulations.

The PDP Law does not contain AI-specific provisions. Nevertheless, the use of AI systems or models involving the processing of personal data is subject to the general requirements under the PDP Law. In particular,

such processing may be classified as high-risk processing, as the use of new or emerging technologies is expressly recognised as one of the indicators of high-risk processing under the PDP Law framework and further triggers the requirement to conduct a DPIA.

In addition, the PDP Law grants data subjects specific rights in relation to automated decision-making. Where a data subject objects to a decision made solely through automated processing, which may include decisions generated automatically through AI, the data subject may request that the decision be reviewed or re-made with human involvement, in accordance with the PDP Law.

1.6 Data Breach Requirement

In the event of a data breach or personal data protection failure, the personal data controller must provide a written notification no later than 3 x 24 hours (ie, within 72 hours) to the affected personal data subject and to the personal data protection authority (“PDP Authority”). In certain cases, where the personal data protection failure interferes with public services and/or has a significant impact on the public interest, the personal data controller must notify the public of such personal data protection failure.

The written notification shall at least contain the following:

- the disclosed personal data;
- when and how the personal data are disclosed; and
- efforts to handle and recover from the disclosure of personal data by the personal data controller.

The PDP Law stipulates that the data privacy litigation or dispute resolution is conducted through court, arbitration, or other alternative dispute resolution bodies.

In practice, a data breach involving ESOs must also be notified to the MOCD within 72 hours from the discovery of the personal data protection incident. The MOCD provides a specific reporting form for data breach/incident, which must be completed by the ESOs and submitted together with relevant supporting documents evidencing the occurrence of the personal data protection breach.

With respect to investigations conducted by the MOCD, the legal basis for such investigative powers is derived from the EIT Law and MOCD Reg 20/2016. Under the EIT Law, the competent authorities, specifically investigators from the MOCD, the Indonesian National Police and certain authorised civil servant investigators, are granted the authority to examine the following:

- the accuracy of reports or information relating to criminal offences in the field of information technology and electronic transactions;
- any person and or business entity reasonably suspected of committing a criminal offence in the field of information technology and electronic transactions; and
- any tools and/or facilities related to information technology activities that are suspected of being used to commit criminal offences in the field of information technology and electronic transactions

Under MOCD Reg 20/2016, the MOCD is authorised to trace and follow up on reports of personal data protection failures and, for supervisory purposes, may request data and information from ESOs in connection with personal data protection, either periodically or at any time as deemed necessary.

1.7 Regulators

PDP Authority

The PDP Law mandates an independent PDP Authority appointed by the President. The PDP Authority has the power to:

- govern and establish policies in the field of personal data protection;
- conduct supervision over the compliance of personal data controllers;
- impose administrative sanctions for violations of personal data protection committed by personal data controllers and/or personal data processors;
- assist law enforcement authorities in handling alleged personal data violations as referred to in the PDP Law;
- co-operate with personal data protection authorities of other countries in order to resolve alleged cross-border personal data protection violations;

- assess the fulfilment of requirements for the transfer of personal data outside the jurisdiction of the Republic of Indonesia;
- issue orders as follow-up to the results of supervision of personal data controllers and/or personal data processors;
- publish the results of personal data protection supervision in accordance with applicable laws and regulations;
- receive complaints and/or reports concerning alleged violations of personal data protection;
- conduct examinations and tracing in relation to complaints, reports, and/or supervisory findings of alleged violations of personal data protection;
- summon and require the attendance of any person and/or public institutions related to alleged violations of personal data protection;
- request explanations, data, information, and documents from any person and/or public institutions in connection with alleged violations of personal data protection;
- summon and require the attendance of experts as necessary for examinations and tracing relating to alleged violations of personal data protection;
- conduct examinations and tracing of electronic systems, facilities, rooms, and/or premises used by personal data controllers and/or personal data processors, including obtaining access to data and/or appointing third parties; and
- request legal assistance from the public prosecutor in the resolution of personal data protection disputes.

As of the date of this guide, the President has yet to appoint the PDP Authority to assume the roles above. Hence, it is also important to identify other authorities who might have mandates based on sectoral regulations.

Sectoral Regulators

Subject to the applicable sectoral laws and regulations, there are sectoral regulators who might have mandates to supervise the personal data processing, as outlined below.

MOCD

The MOCD derives its authority in personal data protection from the EIT Law and GR 71/2019 and cur-

rently serves as the primary supervisory authority for ESOs. Its mandate includes issuing data protection-related regulations for electronic systems, overseeing compliance, conducting investigations and administrative enforcement for violations, and co-ordinating with law enforcement agencies and other relevant sectoral authorities.

OJK

The OJK holds specialised supervisory authority over personal data protection within the financial services sector, covering banks and other financial institutions, financial technology and digital payment providers, capital markets and securities companies, as well as insurance, pension funds, and other non-bank financial service institutions. The OJK conducts regular co-ordination with the MOCD regarding overlapping jurisdictions, particularly for fintech and digital financial services utilising electronic systems.

National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara, BSSN*)

The BSSN is the primary technical authority for cybersecurity aspects of personal data protection in Indonesia, particularly in cases involving cyber incidents, national vital infrastructure, or cross-border cyber threats. Under BSSN Regulation No 1 of 2024 on Cyber Incident Management (“BSSN Reg 1/2024”), ESOs, especially those operating vital information infrastructure, must report cyber incidents to the National Cyber Incident Response Team (Nat-CSIRT) within 24 hours. The BSSN is empowered to conduct technical investigations and digital forensics, identify system vulnerabilities, provide incident containment and recovery assistance, and lead the response to major cyber incidents affecting the security of personal data.

Law enforcement

Law enforcement agencies, including the Indonesian National Police and Attorney General’s Office, possess authority in handling criminal cases related to personal data protection based on (i) criminal sanctions in the PDP Law and (ii) cyber-crimes and criminal sanctions under the EIT Law. Criminal law enforcement is conducted in accordance with the Criminal Procedure Code (KUHP), special procedures in the

EIT Law for cyber crimes, and digital evidence handling protocols.

Law enforcement agencies co-ordinate with the MOCD, the OJK, and the BSSN regarding (i) information exchange for investigation purposes; (ii) technical assistance in digital forensic analysis; (iii) cross-jurisdictional case co-ordination; and (iv) prevention of overlapping legal processes.

Cross-Border Co-Ordination

Pursuant to the cross-border co-ordination, the PDP Law grants the authorities, including the PDP Authority, the power to conduct international co-operation in personal data protection, including: (i) information exchange with foreign data protection authorities; (ii) mutual legal assistance in investigations; (iii) harmonisation of data protection standards; and (iv) joint capacity development.

1.8 Enforcement Proceedings and Fines

The PDP Authority possesses comprehensive investigative powers, including the ability to conduct examinations, request documentation, interview relevant parties, and co-ordinate with other authorities. The PDP Authority may initiate investigations based on data breach notifications, public complaints, audits, or referrals from other government agencies.

Administrative Sanctions

The PDP Law grants the PDP Authority the power to impose administrative sanctions, including written warnings, temporary suspension of personal data processing activities, permanent suspension of processing operations, deletion of personal data, and imposes administrative fines. The PDP Law imposes fines of up to 2% of the annual revenue of the personal data controller or personal data processor in the preceding financial year.

However, as of the date of this guide, the detailed procedures for imposing administrative sanctions, including assessment criteria, severity violations, penalty calculation guidelines, and appeal mechanisms, have not been fully elaborated through implementing regulations. The PDP Law provides the statutory foundation, but operational procedures remain under development by the competent authorities.

Criminal Sanctions

The PDP Law also regulates the criminal sanctions, as follows:

- **Unlawful Collection or Obtaining of Personal Data:** Any person who intentionally and unlawfully obtains or collects personal data that does not belong to them, for their own benefit or the benefit of another person, and which results in loss to the data subject, is subject to imprisonment of up to five years and/or a fine of up to IDR5 billion.
- **Unlawful Disclosure of Personal Data:** Any person who intentionally and unlawfully discloses personal data that does not belong to them is subject to imprisonment of up to four years and/or a fine of up to IDR4 billion.
- **Unlawful Use of Personal Data:** Any person who intentionally and unlawfully uses personal data that does not belong to them is subject to imprisonment of up to five years and/or a fine of up to IDR5 billion.
- **Forgery of Personal Data:** Any person who intentionally creates false personal data or falsifies personal data with the intent to obtain a benefit for themselves or another person, and which causes loss to another person, is subject to imprisonment of up to six years and/or a fine of up to IDR6 billion.

Further, Law No 1 of 2026 on Criminal Sentencing Adjustment introduced a category-based fine system that substantially reduced the monetary penalties. Unlawful collection, disclosure, and use of personal data are now subject to fines capped at IDR200 million, while the forgery of personal data is subject to fines capped at IDR500 million, without any reduction in the applicable prison terms.

Where these offences are committed by or for a corporation, criminal liability may be imposed on both the company and the individuals involved, and corporate fines may be increased by up to ten times the statutory maximum fines applicable to individuals.

1.9 Enforcement Trends

The PDP Law came into effect in October 2024, following the end of the two-year statutory grace period. However, administrative enforcement has not yet been fully implemented, as the PDP Authority mandated by

the PDP Law has not been established. As a result, although the administrative sanctions framework under the PDP Law is formally in force, no formal PDP Authority-led administrative penalties have yet been issued.

Unlike administrative sanctions, criminal sanction enforcement under the PDP Law has been active and there are several court decisions in relation to criminal sanctions in the PDP Law. The first court decision is Karanganyar District Court Decision No 5/Pid. Sus/2023/PN Krg dated 16 March 2023, in which the perpetrator was found guilty of data falsification and imprisoned for four years, and also ordered to pay an IDR1 billion fine.

2. Privacy Litigation

2.1 Privacy Litigation Overview

The number of privacy-related proceedings in Indonesian courts remains relatively low, with the legal framework still developing following the enactment of the PDP Law.

Claimant Types and Legal Standing Issues

The primary category of claimants in privacy-related disputes consists of individual data subjects who have suffered direct harm from personal data processing violations. These individuals typically include affected customers or users following data breaches, unauthorised disclosure incidents, or other forms of personal data protection failure.

The second category of claimants are consumer groups or public interest litigants. However, in practice, significant legal standing challenges have emerged regarding collective or representative actions brought by consumer groups or public interest organisations. The legal standing of such entities to represent broader classes of affected individuals remains debatable under Indonesian procedural law, with courts demonstrating inconsistent approaches to these claims.

Available Remedies Under PDP Law

The PDP Law provides a framework of remedies for data subjects who suffer harm from personal data protection violations, including the right to claim com-

pensation. The mechanism to claim compensation is expected to be further elaborated in the implementing regulation of the PDP Law.

In addition to compensation, the PDP Law allows courts to order injunctive and corrective measures, including requiring the suspension of unlawful data processing, the implementation of appropriate security safeguards, and the correction of inaccurate personal data.

2.2 Recent Case Law

The ongoing enforcement cases have mainly relied on criminal sanctions under the PDP Law and the EIT Law, particularly in cases involving unlawful access, disclosure, or forgery of personal data.

Aside from the criminal cases, there are several constitutional court decisions in Indonesia related to the PDP Law. The landmark decision on the PDP Law is Constitutional Court Decision No 151/PUU-XXII/2024 dated 30 July 2025, which clarifies the interpretation of the fulfilment of criteria requiring a data protection controller or data protection processor to appoint a DPO.

2.3 Collective Redress Mechanisms

Indonesia allows collective redress through class actions under Supreme Court Regulation No 1 of 2002 on Class Action Procedure. This mechanism permits one or more plaintiffs to represent a larger group with common facts and legal issues. In principle, personal data protection violations may be pursued through this mechanism.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Indonesia does not currently have a single, comprehensive legal framework specifically governing the protection and processing of non-personal data. Instead, the regulation of non-personal data is primarily fragmented into several sectoral laws.

By way of example, in the electronic ecosystem, the relevant regulations include (among others) GR

71/2019, Government Regulation No 80 of 2019 on Electronic Commerce, MOCD Regulation No 5 of 2020 as amended by Minister of Communication and Informatics Regulation No 10 of 2021 on Private Electronic System Providers (“MOCD Reg 5/2020”), and applicable cybersecurity regulations. In the financial sector, among others, OJK Regulation No 44 of 2024 on Bank Secrecy, OJK Regulation No 22 of 2023 on Consumer and Public Protection in the Financial Services Sector and BI Regulation No 3 of 2023 on BI Consumer Protection also apply. There are also archival and record-keeping laws, including Law No 8 of 1997 on Company Documents (“Company Documents Law”) and Law No 43 of 2009 on Archives.

In general, these regimes regulate data management throughout its life cycle without distinguishing between personal and non-personal data, including data governance and use, security and confidentiality, sector-specific handling requirements, archiving and retention periods, data transfers, and incident or breach response obligations, including reporting timelines and notifications to relevant sectoral authorities. Where certain regulations make reference to personal data, their interaction with the PDP Law is addressed in **3.2 Interaction of Data Regulation and Data Protection**.

3.2 Interaction of Data Regulation and Data Protection

The interaction between sectoral regulations and the PDP Law generally takes two forms. First, certain sector-specific regulations expressly refer to the PDP Law for personal data protection compliance. Second, other regulations impose additional, supplementary, or more specific personal data processing requirements in respect of particular categories of data or regulated activities. For example, while the PDP Law does not expressly regulate data retention periods, such requirements may be addressed under applicable sectoral regulations (eg, under the Company Documents Law, records, bookkeeping evidence, and supporting financial administrative data must be retained for a period of ten years, calculated from the end of the relevant company’s financial year).

In essence, sector-specific data handling rules are applicable in parallel with the PDP Law, provided

they do not conflict with its provisions. Where data qualifies as personal data, the PDP Law operates as the primary legal framework, while sectoral regulations typically supplement the PDP Law by regulating sector-specific processing scenarios or imposing heightened obligations.

3.3 Rights and Obligations Under Applicable Data Regulation

The applicable rights and obligations largely depend on the relevant sector and regulatory context. In practice, contractual arrangements also play a critical role in allocating rights, obligations, and liability.

Organisations should therefore ensure that their contracts clearly define the agreed arrangements, including, among others, roles and responsibilities of each party in relation to the data and its processing, permitted uses or purposes, and applicable technical and organisational measures, while also ensuring the inclusion of provisions addressing compliance with any applicable sector-specific regulatory requirements.

3.4 Regulators and Enforcement

In relation to non-personal data, enforcement authority depends on the nature of the data and the relevant sector. Competent authorities include, among others, the MOCD for ESOs, the OJK for the financial services sector, and the BSSN for cybersecurity matters.

Co-ordination among regulators typically arises in practice where incidents affect both non-personal and personal data. In such cases, sectoral regulators may co-ordinate with the personal data protection authority under the PDP Law, as well as with other relevant government bodies, depending on the affected sector.

A notable recent trend is the increasing frequency and sophistication of cybersecurity incidents in various sectors, which require more active inter-agency co-ordination, particularly where an incident affects both personal and non-personal data and simultaneously implicates data protection, system security, and sector-specific compliance obligations.

4. Sectoral Topics

4.1 Use of Cookies

Indonesia does not currently have a specific regulation that expressly governs the use of cookies, software development kits (SDKs), or other online tracking technologies.

However, to the extent that such technologies involve the processing of personal data, their use is subject to the general principles and requirements under the PDP Law and the EIT Law, including to provide clear information and transparency to data subjects regarding the collection and use of their personal data in such cookies.

4.2 Personalised Advertising and Other Online Marketing Practices

The PDP Law does not specifically regulate personalised or targeted advertising activities. However, where such activities involve the processing of personal data or profiling activities, they are subject to the general principles and requirements under the PDP Law.

Given the absence of specific provisions governing personalised advertising or marketing, the applicable marketing requirements must be assessed on a sectoral basis. For instance, in the financial services sector, OJK Reg 22/2023 prohibits financial services business actors from offering products and/or services to prospective consumers and/or consumers through personal communication channels without the consent of prospective consumers and/consumers.

In the electronic ecosystem, particularly under PP TUNAS, ESOs that are potentially directed at or intended for children are prohibited from conducting profiling by default, by any means or methods, including for product or service offerings or other purposes. Where profiling is to be carried out, it must be justified through a risk assessment or demonstrated to be essential for the provision of the service.

4.3 Employment Privacy Law

There are currently no employment-specific personal data protection laws. The processing of employees' personal data is therefore subject to the PDP Law and its implementing regulations.

Employee-related processing activities, including employee monitoring, are not specifically prohibited, provided that they are conducted in accordance with the PDP Law, and are typically grounded in contractual arrangements between the employer and the employee.

In current practice, employers in Indonesia commonly rely on employment agreements as the primary lawful basis for processing employee personal data, without prejudice to the availability of other lawful basis under the PDP Law for specific employee-related data processing activities.

4.4 Data Protection in M&A

The PDP Law regulates personal data protection requirements in the context of corporate actions, including mergers, acquisitions, spin-offs, and dissolutions. Under the PDP Law, a personal data controller in the form of a legal entity that undergoes a merger, acquisition, spin-off, and/or dissolution is required to notify personal data subjects of the personal data transfer both prior to and after the completion of such corporate action.

In the event that a personal data controller in the form of a legal entity is dissolved or liquidated, the storage, transfer, deletion, or destruction of personal data must be carried out in accordance with applicable laws and regulations, and such actions must be notified to the relevant personal data subjects.

Further procedural details are expected to be regulated under the forthcoming government regulation implementing the PDP Law.

In practice, notifications to data subjects may be delivered through any medium that is reasonably accessible to them. For example, in the context of an acquisition where Indonesian corporate law requires pre- and post-acquisition announcements to be published in national newspapers, PDP-related notifications may be incorporated into such mandatory corporate announcements, provided that it is made clear that the announcement is also addressed to data subjects, and not solely to creditors.

Accordingly, each corporate action must be assessed on a case-by-case basis to determine whether the role of the personal data controller remains unchanged, is transferred to another entity, or is otherwise impacted.

5. International Considerations

5.1 Restrictions on International Data Transfers

Under the PDP Law, a cross-border transfer of personal data occurs where a personal data controller or personal data processor makes personal data available or provides access to another party located outside the jurisdiction of Indonesia, whether by transmission, remote access, hosting, or any other technical means. This includes cloud hosting, cross-border access to databases, and sharing of data with overseas affiliates or vendors.

Based on PDP Law, cross-border transfers of personal data are permitted only if one of the following safeguards is satisfied:

- **Adequacy Principle:** A transfer is permitted where the recipient country or international organisation provides a level of personal data protection that is equal to or higher than that under Indonesian law.
- **Contractual Safeguards:** Where the recipient country does not provide an equivalent level of protection, a transfer may still take place if the personal data controller or processor implements binding contractual safeguards that ensure the protection of personal data in accordance with the PDP Law.
- **Consent of the Data Subject:** If neither adequacy nor contractual safeguards can be satisfied, a cross-border transfer may still be carried out based on the consent of the personal data subject.

Cross-border transfers of non-personal electronic data are governed by GR 71/2019, which allows private ESOs to host, process, store electronic systems and electronic data (including non-personal data) outside the territory of Indonesia, except for the financial sector, which is subject to sectoral regulations.

5.2 Government Notifications and Approvals

The PDP Law does not stipulate a prior approval requirement by PDP Authority for international personal data transfers. However, the PDP Law grants the PDP Authority specific powers to conduct assessments of cross-border data transfer requirements for fulfillment.

In relation to the electronic system, private ESOs are obligated to co-ordinate with MOCD in relation to international transfers.

The regulatory requirements in relation to international transfers may be subject to sectoral laws, among others:

- **Digital Financial Asset (Including Crypto-Assets):** OJK Regulation No 27 of 2024 on the Organisation of Trading of Digital Financial Assets including Crypto Assets (“OJK Reg 27/2024”) establishes specific requirements for personal data handling within the digital asset sector, though it does not explicitly stipulate comprehensive cross-border data transfer procedures. However, the regulation mandates that any transfer of data subjects’ personal data to third parties must be notified to the OJK.
- **Healthcare:** Government Regulation No 28 of 2024 concerning Health (“GR 28/2024”) establishes stringent authorisation requirements for international transfers of health-related personal data, that cross-border transfers of health data must obtain prior approval from the Minister of Health of the Republic of Indonesia, which applies to all categories of health data transfers, including patient records, medical research data, pharmaceutical information, and public health surveillance data.
- **Banking and Financial Services:** Bank Indonesia Regulation No 23/6/PBI/2021 on Payment Systems allows payment transaction processing to be conducted outside the territory of the Republic of Indonesia, provided that prior approval is obtained from Bank Indonesia. Such approval may be granted by taking into account, among others, the use of electronic systems and/or operational activities integrated with the principal office of the payment service provider located outside Indonesia, the

readiness of national industry and infrastructure, and other factors determined by Bank Indonesia.

5.3 Data Localisation Requirements

In general, the PDP Law does not require data localisation. Remote access from abroad is generally treated as a cross-border data transfer and is therefore subject to the PDP Law transfer safeguards.

The following are some sectors in which data localisation is mandatory or required:

- **Healthcare:** GR 28/2024 requires health data and health information systems to be stored and processed in data centres located within Indonesian jurisdiction. This includes hospitals, clinics, digital health platforms, and other healthcare service providers.
- **Banking:** OJK Regulation No 11 of 2022 (“OJK Reg 11/2022”) establishes comprehensive data localisation obligations for the banking sector. This provision mandates that both primary data centres and disaster recovery centres must be located within Indonesian territory, ensuring complete domestic control over critical banking infrastructure.
- **Digital Financial Asset (including Crypto-Assets):** OJK Reg 27/2024 and Government Regulation No 49 of 2024 on the Implementation of Crypto Asset Trading (“GR 49/2024”) require crypto-asset service providers to maintain both their data centres and disaster recovery centres within Indonesian territory, thereby imposing comprehensive data localisation and infrastructure residency obligations.
- **Financial Technology:** OJK Regulation No 3 of 2024 on the Implementation of Financial Technology Innovation and Aggregation Services (“OJK Reg 3/2024”) establishes specific data localisation obligations for the financial technology sector, including payment system aggregators and technological innovation organisers in financial services. OJK Reg 3/2024 requires that data centres and data recovery centres be located within Indonesia, ensuring domestic control over fintech data infrastructure.

- **Non-Bank Financial Institutions:** OJK Regulation No 4 of 2021 (“OJK Reg 4/2021”) imposes data localisation requirements on non-bank financial institutions, including insurance companies, pension funds, financing institutions, and other non-bank financial service providers, requiring relevant data processing infrastructure to be located within Indonesian territory.

5.4 Blocking Statutes

Although the PDP Law does not contain blocking provisions against foreign courts, MOCD Reg 5/2020 authorises the government to implement access blocking of electronic systems. Under these regulations, MOCD can block access to a private ESO if:

- the private ESO fails to grant access to its systems or data for domestic law enforcement or regulatory oversight;
- the system facilitates the distribution of content deemed prohibited under Indonesian law; or
- the private ESO fails to meet the mandatory registration requirements.

5.5 Recent Developments

The more detailed requirements on international data transfer are expected to be regulated under the upcoming Government Regulation regarding the implementation of PDP Law, including formal criteria for assessing foreign data protection regulation, standards for data transfer agreements, binding corporate rules, and requirements for transfer impact assessments.

Trends and Developments

Contributed by:

Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur
ABNR Counsellors at Law

ABNR Counsellors at Law was founded in 1967. It is Indonesia's longest-established law firm and has played a pivotal role in shaping the development of international commercial law in the country, particularly during its economic reopening to foreign investment in the 1960s. Today, with a team of around 120 legal professionals – including 27 partners and three foreign counsels – ABNR stands as Indonesia's largest independent, full-service law firm. The firm is proud

to have female partners, reflecting its commitment to diversity and inclusion. ABNR has consistently maintained its position as a top-tier law firm since its establishment. As the exclusive Indonesian member of Lex Mundi since 1991 – the world's leading network of independent law firms with representation in over 100 countries – ABNR provides seamless global reach for its clients.

Authors



Agus Ahadi Deradjat (Agung) is a partner at ABNR and a former member of the firm's management board. Agung focuses his practice on corporate/M&A, foreign direct investment (FDI), and TMT. He

advises leading domestic and multinational corporations across all leading industries and sectors, but offers particular expertise and experience in life sciences, technology and telecommunications, e-commerce and automotive. Agung has worked on a number of major M&A and FDI transactions for high-end multinational clients, as well as significant FDI transactions in the technology, pharma industry, manufacturing, chemicals, and the natural resources sectors. Agung is ranked for TMT (Band 1) and corporate and M&A by Chambers Asia-Pacific.



Mahiswara Timur joined ABNR as an associate in June 2015 and was made partner in January 2026. Timur focuses on IT-related assignments such as telecommunications networks (including for submarine cables and

satellites) and services, cybersecurity, privacy and personal data protection, digital content compliance, cloud computing, e-commerce, broadcasting,

over-the-top services, data centre operation, digital platforms and services in Indonesia, the internet of things, and online games. He has advised start-up clients and leading multinational technology, social media and streaming companies. His extensive understanding of the regulatory, technical and practical aspects of the TMT business has enabled Timur to provide precise, comprehensive advice as well as practical solutions well-tailored to client needs and business operations.



Nina Cornelia Santoso joined ABNR in April 2015 and became a senior associate in January 2022. Nina's main areas of professional practice encompass TMT, competition, M&A, and FDI. In TMT, she regularly advises

high-profile multinationals and local companies on privacy and data protection, internet-based products and services (digital platforms, social media, online games, cloud computing, e-commerce, over-the-top services), cybersecurity, and content moderation. She occasionally advises clients on telecommunications networks and services matters (including subsea cables). Her graduate studies at the University of Cambridge provide her with a deep understanding of the EU General Data Protection Regulation (GDPR).

INDONESIA TRENDS AND DEVELOPMENTS

Contributed by: Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur,
ABNR Counsellors at Law



Dhan Partap Kaur (Sonia) is an associate at ABNR whose practice focuses on TMT, M&A, and general corporate law. In the TMT sector, Sonia regularly advises leading multinationals and local companies on data privacy and protection, internet-based services (digital platforms, social media, online games, cloud computing, e-commerce, and over-the-top services), cybersecurity, and content moderation. She is known for delivering tailored, practical solutions aligned with each client's business objectives and frequently provides hands-on support to clients navigating complex regulatory frameworks.

ABNR Counsellors at Law

Graha CIMB Niaga
24th Floor
Jl. Jenderal Sudirman Kav. 58
Jakarta
12190
Indonesia

Tel: +62 21 250 5125/5136
Fax: +62 21 250 5001
Email: info@abnrlaw.com
Web: www.abnrlaw.com



COUNSELLORS AT LAW

Indonesia's Evolving Data Protection Framework: Key Developments in AI, Cyber Resilience and Child Protection

PDP Law in a nutshell

Law No 27 of 2022 on Personal Data Protection (the "PDP Law") serves as the overarching law on personal data protection in Indonesia. In addition to the PDP Law, the implementation of personal data protection is subject to the following laws and regulations:

- the PDP Law;
- Law No 11 of 2008 on Electronic Information and Transactions, last amended by Law No 1 of 2024 (the "EIT Law");
- Government Regulation No 71 of 2019 on the Provision of Electronic Systems and Transactions ("GR 71/2019"); and
- other sector-specific regulations.

The PDP Law has extraterritorial effect, meaning that overseas organisations, including individuals, public entities, and international organisations, can be prosecuted in Indonesia for violating the law, particularly for non-compliance in processing personal data of Indonesian citizens, whether onshore or offshore. The Indonesian government has been working on the Draft Implementing Regulation for Law No 27 of 2022 on Personal Data Protection ("Draft GR PDP"), which is intended to provide further guidance on the law's implementation and enforcement. However, as of early 2026, there is no clear timeline for its finalisation. Based on the latest available public statement from the Ministry of Communications and Digital Affairs (MOCD) in October 2025, the Draft GR PDP has completed its harmonisation process, and has been passed to the State Secretary for approval by the President.

Furthermore, an amendment to the current PDP Law is currently included in the Annual Priority National Legislation Programme (which is prepared jointly by the House of Representatives, the Regional Representatives Board, and the President) for 2026. The amendment was registered on 23 September 2025 and is only at the planning stage.

Some of the notable provisions under the PDP Law are outlined below.

Types of personal data

The PDP Law defines "personal data" as "any data related to an individual (natural person), whether identified or capable of being identified independently or in combination with other information, whether directly or indirectly, through the use of an electronic system and/or non-electronic means". The individual is referred to as a "data subject".

The PDP Law further categorises personal data as general personal data (name, gender, nationality, religion, marital status, or personal data that together can identify a person) and specific personal data (data on health, biometric or genetic, and criminal records; data on children; financial data; and/or other data in accordance with the laws and regulations). There is no particular differentiation in treatment of the processing of general or specific personal data. However, the processing of specific personal data would trigger additional obligations, such as the need to perform a Data Protection Impact Assessment (DPIA) and appoint a Data Protection Officer (DPO).

Lawful basis for processing of personal data

The PDP Law acknowledges several legal bases for personal data processing: (i) consent; (ii) contractual necessity; (iii) compliance with a data controller's legal obligations; (iv) protection of the vital interests of the data subject; (v) public interest, for the provision of public services or for the exercise of lawful authority; and (vi) legitimate interest. We observe that the above legal bases are very similar to the concept adopted by the EU GDPR.

Cross-border data transfer

The PDP Law introduces layered requirements to allow data controllers to transfer personal data outside Indonesian territory, namely:

- (i) The country receiving the transfer of personal data has an equal or higher level of personal data protection than afforded under the PDP Law ("Adequacy of Protection").
- (ii) In the absence of Adequacy of Protection, an adequate level of binding personal data protection must be available ("Appropriate Safeguards").
- (iii) In the event that neither Adequacy of Protection nor Appropriate Safeguards are present, consent

for the cross-border data transfer must be given by the data subject.

Points (i) to (iii) above must be assessed and implemented in sequence. To date there is no indication that an official approved list of countries that meet the Adequacy of Protection requirements will be published.

Data Protection Authority (DPA)

The PDP Law mandates the formation of a DPA that is tasked to act as regulator, supervisor, and executor in data protection matters by the President, which is yet to be formed. In the meantime, pursuant to MOCD Regulation 1/2025 on Organisation and Work Procedures, matters concerning personal data protection are currently under the authority of Directorate General of Digital Space Supervision at the MOCD (DG). The DG is tasked with formulating and implementing policies related to digital space supervision and personal data protection. Based on statements made by the current Minister in public announcements, the DPA is expected to be established in the near future.

DPO

The PDP Law requires a data controller or data processor to appoint a DPO in situations where: (i) it processes personal data for public interest; (ii) the data controller's core activities have such a nature, scope, and/or purpose that require regular and systematic monitoring of personal data on a large scale; and (iii) the data controller's core activities involve large-scale processing of specific/sensitive or criminal-related personal data.

The Indonesian Constitutional Court, through Decision No 151/PUU-XXII/2024 dated 30 July 2025, held that this cumulative reading was unconstitutional. The word “and” the PDP Law must instead be read as “and/or,” meaning that fulfilling any one of these conditions is sufficient to trigger the obligation to appoint a DPO. Thus, data controllers and data processors should reassess their obligations under the PDP Law to appoint a DPO.

Development on artificial intelligence (AI)

AI is increasingly being adopted across multiple sectors in Indonesia, including by government institutions

in their daily operations. Recognising the growing demand for AI technologies, the government has indicated its support for AI development and is planning to accommodate its use through forthcoming regulations and infrastructure initiatives.

While Indonesia has yet to introduce binding regulations governing the use of AI, MOCD issued Circular Letter No 9 of 2023 on Ethics of Artificial Intelligence (“CL 9”). As of early 2026, CL 9 remains the only general regulatory guidance addressing the use of AI by business undertakings.

In summary, CL 9 contains the following salient items:

- general definitions, general guidelines for values, ethics, and control of consulting, analysis and programming activities with an AI basis by business undertakings and electronic systems operators (ESOs);
- emphasis that the CL 9 is applicable to: (i) business undertakings operating under Indonesian Standard Business Classification (KBLI, similar to ISIC) 62015 on AI-Based Programming Activities; (ii) ESOs in public scope; and (iii) ESOs in private scope; however, with the issuance of KBLI 2025 version, KBLI 62015 is no longer applicable (AI-based programming activity is now encompassed under several different KBLIs, which are the issuance of AI-based software under KBLI 58290 (Other Software Publication) and development of AI fundamental components under KBLI 62194 (Activities for Developing Fundamental Components of Artificial Intelligence)); and
- emphasis on ethical use of AI by adhering to the principles of inclusivity, humanity, safety, accessibility, transparency, credibility and accountability, personal data protection, sustainable development and environment, and protection of intellectual property.

Additionally, the Financial Services Authority (*Otoritas Jasa Keuangan*, or OJK) has issued a Code of Ethics for Responsible and Trustworthy AI in the Financial Technology Industry, which applies to financial technology providers. The Code also stipulates principles of AI utilisation in the financial services industry, which includes: beneficial, fair and accountable, transpar-

ent and explicable, and robust and secure principles. In the banking sector, the OJK has issued Artificial Intelligence Governance for Indonesian Banking, which provides guidance for Indonesian banks on the responsible development and deployment of AI and reiterates the application of these principles in banking activities.

In response to the increasing demand for AI-related regulations and infrastructures, the MOCD recently issued its Whitepaper Roadmap for AI (“AI Roadmap”), which includes the MOCD’s intention to support the development of AI and ways to optimise AI as part of Indonesia’s digital ecosystem development. The AI Roadmap includes the MOCD’s five-year programmes and goals related to the development of AI, including the intention to conduct research on AI, create regulations and policies regarding the use of AI, building AI infrastructures, and conducting harmonisation and standardisation on the interoperability of AI systems used in ministries and institutions. The AI Roadmap also addresses personal data protection aspects in the development, uses, and operation of AI.

Update on cyber resilience

Pursuant to the Indonesian Cyber Security Landscape published by the National Cyber and Crypto Agency in 2024, there were 56,128,160 data exposures that affected 461 stakeholders in Indonesia. As of August 2025, the National Cyber and Crypto Agency (BSSN) recorded a total of 3.64 billion cyber-attacks. Recurring data breaches in Indonesia highlight vulnerabilities in the country’s cybersecurity policies and systems, along with insufficient supervision and enforcement against perpetrators.

The current legal framework requires reporting data breaches to the MOCD and notifying data subjects, while cybersecurity incidents without a data breach must be reported to regulators and law enforcement. Below are the regulatory regimes for data breach and cybersecurity incident notification:

- PDP Law: Upon “failure to protect personal data”, the data controller must notify both the affected data subject and the Data Protection Authority within 72 hours. This includes breaches that impact confidentiality, integrity, or availability of personal

data, resulting in destruction, loss, alteration, or unauthorised access.

- Electronic System Operation Regulations (GR 71/2019): An ESO must: (i) report to relevant authorities and law enforcement if there is a serious system failure due to third-party interference, and (ii) notify data subjects if personal data protection fails within its system.

The BSSN has issued BSSN Regulation No 1 of 2024 on Cyber Incident Management (“BSSN Reg. 1/2024”) in an effort to combat the high number of cyber incidents, establishing Cyber Incident Response Teams (CIRTs) at a national, sectoral, and organisational level. CIRTs are expected to manage cyber incidents through the following steps:

- handling of cyber incidents;
- mitigation and recovery from cyber incidents; and
- reporting and dissemination of cyber incident information.

The membership of the national CIRT consists of representatives from:

- the BSSN;
- ministries or institutions;
- state-run institutions owning and/or operating vital information infrastructure (IIV); and
- ESOs other than state-run institutions owning and/or operating IIV.

Ministries and institutions are also required to create their own sectoral CIRT, while state-run institutions owning and/or operating IIV and ESOs other than state-run institutions owning and/or operating IIV are required to form an organisational CIRT.

The government is also preparing the Draft Regulation for Cyber Security and Resilience (“Cybersecurity Bill”), which is intended to strengthen national cybersecurity protection. This Bill will regulate information infrastructure providers, critical information infrastructure, and digital product/service providers to implement stricter cybersecurity standards by combining upstream (requirements), midstream (monitoring, evaluation, and assessment/reporting), and downstream (sanctions) approaches.

Based on the publicly available draft, the key points in the Cybersecurity Bill include the following:

- Relevant entities are encouraged to report cyber incidents within a certain timeframe, with a view to facilitating improvement and mitigation measures rather than imposing sanctions.
- It mandates the implementation of security standards throughout the digital product process to protect national infrastructure from cyber threats.

The Cybersecurity Bill is expected to be the legal basis for maintaining Indonesia's cybersecurity, sovereignty, and resilience amidst escalating global threats, complementing the existing EIT Law. On the House of Representatives' website, the Bill is only registered in the Medium-Term Annual Priority National Legislation Programme (2025-2029), and was last updated in November 2024. However, based on news articles in August 2025, the Bill is currently at the harmonisation stage, where the draft is deliberated among various ministries/agencies and relevant stakeholders.

Likely implementation of the Draft GR PDP

As noted above, the Indonesian government has been preparing the Draft GR PDP for some time. While it is expected to provide further guidance on the implementation of the PDP Law, the regulation has yet to be issued. In addition, the Draft GR PDP contemplates the conferral of certain regulatory powers on the DPA, which has not yet been established.

Some notable provisions under the Draft GR PDP (latest publicly available draft as of August 2023) are outlined below.

Requirements for reliance on lawful bases

The Draft GR PDP provides further guidance or requirements on reliance upon lawful bases of processing, including:

- **Express Consent:** If the data subject refuses to provide consent, the data controller cannot deny goods or services to the data subject, provided no personal data processing is involved. Additionally, the data controller must implement measures to identify users and ensure relevant personal data

protection, including for services targeting children and individuals with disabilities.

- **Contractual Necessity:** In relying on contractual necessity, the agreement that serves as a basis for the personal data processing must: (i) obtain valid express consent from the data subject; (ii) fulfil relevant personal data protection measures; (iii) assess the risk impact on the data subject; (iv) balance interests between the data subject and controller; and (v) acknowledge the data subject's rights. If the data subject does not provide valid consent, the personal data processing is considered null and void.
- **Legitimate Interest:** This lawful basis can be relied upon if the data controller: (i) analyses the needs, objectives, and balance between the rights of data subjects and its own interests, demonstrating a legitimate interest in processing personal data, and (ii) assesses that processing for other legitimate interests does not harm or impact the data subject, ensuring steps are taken to reduce any potential impact.

Practical challenges arising from the existence of various lawful bases for data processing include the need for data controllers to appropriately identify the correct lawful basis for each processing activity. Given that the PDP Law lacks sufficient guidance, data controllers must exercise caution when identifying the purpose of data processing and selecting the appropriate lawful basis. This task requires careful assessment to ensure compliance with the law and to avoid potential risks associated with unlawful data processing. Therefore, it is advisable for data controllers to engage in continuous consultation with authorities or legal consultants to ensure proper understanding and implementation of the law, as well as to address any ambiguities or uncertainties related to the lawful bases for personal data processing.

AI technology providers and users must consider the use of personal data for AI learning, output creation, and feedback. The processing of personal data using AI must: (i) adhere to data protection principles under the PDP Law; (ii) rely on an appropriate lawful basis for processing; and (iii) implement safeguards throughout the processing stages. For instance, users of generative AI platforms must ensure they have secured the

necessary lawful basis, such as obtaining consent from individuals before processing their personal data on AI platforms.

Cross-border data transfer

As stated above, the PDP Law provides that a data controller may transfer personal data offshore should they fulfil the layered requirements of Adequacy of Protection, Appropriate Safeguards, or consent of the data subjects. Data controllers are expected to be fully responsible for implementing appropriate security measures in the processing of data transfer.

The Draft GR PDP determines the Adequacy of Protection for personal data transfers by assessing the recipient country's circumstances, including the existence of (i) personal data protection laws; (ii) a supervisory authority; and (iii) international commitments or obligations under legally binding conventions or resulting from participation in multilateral systems. The Data Protection Authority will compile the list of approved countries.

When using Appropriate Safeguards for transferring personal data abroad, the Draft GR PDP allows safeguards such as (i) agreements between the sender's and recipient's countries; (ii) standard contractual clauses; (iii) binding company regulations for a group; or (iv) other recognised instruments. Data controllers and processors must also meet additional obligations, such as recording the transfer cycle, mapping its implications, and ensuring that the transferred data is sufficient, relevant, and limited to the transfer's purpose.

In July 2025, the MOCD issued a press release on data transfer clauses in a Joint Statement on Framework for United States–Indonesia Agreement on Reciprocal Trade with the United States issued by the White House on 22 July 2025 (“Joint Statement”) with the intention to remove the barrier in digital information trade. The Joint Statement stipulates that Indonesia will provide certainty regarding the ability to transfer personal data out of its territory to the United States. This statement raised concerns over the potential removal of barriers to cross-border personal data transfers, as this could undermine the level of personal data protection and appear inconsistent with

the layered cross-border transfer requirements under the PDP Law. However, the MOCD assured that the Joint Statement is not a form of free transfer of personal data and that transfers will still be conducted based on Adequacy of Protection under Indonesian law. There is currently no further clarification on the implementation of such barrier removal for data transfers with the USA.

Online Child Protection Government Regulation

Government Regulation No 17 of 2025 on the Governance of Child Protection in the Operation of Electronic Systems focuses on mitigating the negative impacts of the digital space for children (“GR 17/2025”). Under GR 17/2025, “children” is defined as anyone under 18 years old.

GR 17/2025 outlines the responsibilities of ESOs in managing online products, services, or features, overseeing child protection governance in electronic systems, and enforcing administrative sanctions. It applies to ESOs that develop or operate internet-connected products, services, or features, such as websites, mobile apps, social media platforms, or gaming services.

Regarding children's personal data protection, GR 17/2025 addresses the following.

DPIA for children

ESO must conduct a DPIA for any online product, service, or feature accessible to children before it is used by them. The DPIA should cover the processing activities, the provider's interests, the necessity and proportionality of the processing, a risk assessment for children's protection, and risk mitigation measures. Additionally, the ESO must maintain the DPIA documentation for as long as the product, service, or feature remains accessible to children, and include a plan to address identified risks before marketing the product.

Obligation to protect children's personal data

ESO must provide clear information on minimum age requirements and implement technical and operational measures to ensure appropriate age verification for children using online products, services, or features, and establish reporting mechanisms to challenge or

adjust age verification decisions and address misuse of such online products, services, or features that violate or may violate children's rights. These measures should align with specified risks and protect children's personal data, secure electronic systems, and prevent unauthorised breaches. Data collected for age verification should only be used for that purpose and deleted once the age requirement is met. ESOs must also ensure that parental/guardian consent has been obtained for all processing of children's data. There are no exceptions to the requirement to obtain parental or guardian consent for the use of children's personal data.

Additionally, ESOs are prohibited from using children's personal data in ways that could harm their physical, mental, or overall well-being, and from developing products that encourage excessive data collection. Data should only be processed if necessary for the service, unless there is a strong reason in the child's best interest. Providers are also banned from using children's data for other purposes without justifiable cause. Lastly, ESOs must appoint a DPO to oversee compliance with child data protection laws and regulations.

The MOCD also passed MOCD Regulation No 9 of 2026 on 6 March 2026 on the Implementation of GR 17/2025. Through the MOCD Reg. 9/2026 press release, the MOCD stated that children under the age of 16 are no longer eligible to create accounts on high-risk platforms as of 28 March 2026. Implementation will be conducted in a gradual manner, starting with platforms such as YouTube, TikTok, Facebook, Instagram, Threads, X, Bigo Live, and Roblox.

Furthermore, there are additional key points as follows:

- **Self-Assessment of Age Categories:** ESOs are to conduct a mandatory self-assessment to ensure that the products, services, and features developed and/or operated by the ESO are in accordance with the minimum age limit of children and the applicable child age group classifications.
- **Child Protection Design:** ESOs are required to have and implement a child protection design to ensure that content accessible to children in the products,

services, and features complies with the minimum age limit for children and the age group classifications of children and does not conflict with laws and regulations.

- **Risk Profile Classification and Mitigation:** MOCD Re. 9/2026 introduces the minimum indicators of risk profile categories, and ESOs' obligation to implement mitigation in relation to the risks.

Roles of DPOs in Indonesia

The PDP Law mandates that both data controllers and processors appoint an officer or staff member to oversee personal data protection functions and ensure compliance with regulations. Since the law's enactment, the number of DPOs in Indonesia has increased, along with the formation of DPO associations. To standardise DPO competencies, the Minister of Manpower issued Decree No 103 of 2023, setting National Competency Standards for Personal Data Protection. These standards guide authorities in developing qualifications, training, and certification for DPOs. However, there is no requirement to register DPOs with authorities.

The government is also actively making efforts to conduct occupational mapping in the information and communication technology field (which encompasses functional areas such as IT governance (including DPOs and Data Protection Executives)), digital product development, etc) through Decree of the Head of the Communication and Digital Human Resources Development Agency of MOCD No 8 of 2025 on the National Occupational Map, as amended by Decree No 45 of 2025. The decree details qualifications, scope of work, tasks and authorities, and is intended to ensure the equal spread of occupation in personal data protection in each functional area.

Suggested approach to establish compliance in Indonesia

Business undertakings should adopt a risk-based approach, which involves identifying, assessing, and managing potential risks associated with personal data processing. Rather than treating all risks equally, businesses should allocate resources to areas that present the greatest threat to data security and privacy, ensuring efforts are proportionate to the risks

Contributed by: Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur,
ABNR Counsellors at Law

involved. In doing so, organisations can prioritise the most critical compliance requirements effectively.

While there are currently fewer privacy-specific regulations on the use of AI, business undertakings in these sectors must still ensure compliance with the PDP Law. Business undertakings must also reassess their current cybersecurity measures in anticipation of the enactment of the Cybersecurity Bill, and ensure compliance with emerging child protection requirements in the digital space.

In light of the anticipated regulatory developments, business undertakings should closely monitor further updates to ensure timely awareness of any changes. This approach will allow business undertakings to take the necessary steps to anticipate any significant changes that may be introduced by the government from time to time. Early identification of material developments will allow sufficient time to implement the necessary compliance measures, thereby minimising operational risk and associated costs.



Law and Practice

Contributed by:

Dan Or-Hof, Eran Gandman, Netanel Aharon and Matan Adar
Or-Hof Law

Contents

1. Legal and Regulatory Framework p.181

- 1.1 Overview of Data and Privacy-Related Laws p.181
- 1.2 Rights and Obligations p.182
- 1.3 Special Categories of Personal Data p.183
- 1.4 Processing of Personal Data for Research and Development Purposes p.184
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.184
- 1.6 Data Breach Requirement p.185
- 1.7 Regulators p.186
- 1.8 Enforcement Proceedings and Fines p.186
- 1.9 Enforcement Trends p.187

2. Privacy Litigation p.187

- 2.1 Privacy Litigation Overview p.187
- 2.2 Recent Case Law p.188
- 2.3 Collective Redress Mechanisms p.188

3. Requirements for the Protection and Processing of Non-Personal Data p.189

- 3.1 Objectives and Scope of Data Regulation p.189
- 3.2 Interaction of Data Regulation and Data Protection p.190
- 3.3 Rights and Obligations Under Applicable Data Regulation p.190
- 3.4 Regulators and Enforcement p.191

4. Sectoral Topics p.192

- 4.1 Use of Cookies p.192
- 4.2 Personalised Advertising and Other Online Marketing Practices p.192
- 4.3 Employment Privacy Law p.193
- 4.4 Data Protection in M&A p.194

5. International Considerations p.195

- 5.1 Restrictions on International Data Transfers p.195
- 5.2 Government Notifications and Approvals p.196
- 5.3 Data Localisation Requirements p.196
- 5.4 Blocking Statutes p.197
- 5.5 Recent Developments p.197

Or-Hof Law is a leading Israeli boutique law firm specialising in data protection, privacy, cybersecurity and AI regulation. The firm advises organisations on navigating complex regulatory and governance challenges at the intersection of law, technology and business, with a strong focus on practical, implementation-oriented solutions. Or-Hof Law works closely with technology companies, multinational corporations, start-ups and regulated entities, supporting them in building compliant and resilient data governance frameworks. The firm is particularly recognised

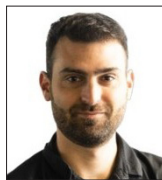
for its hands-on approach to privacy and cyber risk management, regulatory readiness, and cross-border data protection matters. The firm is led by Advocate Dan Or-Hof, a prominent figure in the Israeli and international privacy community, who serves as the IAPP Country Leader for Israel. Under his leadership, Or-Hof Law combines deep regulatory expertise with a business-minded, boutique practice model, offering tailored advice and close partner-level involvement on all matters.

Authors



Dan Or-Hof is a dual-qualified New York and Israeli attorney with an LLM from UC Berkeley and Tel Aviv University. He founded Or-Hof Law in 2013. Recognised by Chambers and Partners for his IT and data protection

expertise, he is regarded as an international data protection leader and is a Westin Fellow Emeritus, 2022 IAPP Global Vanguard Award winner, and the IAPP Country Leader for Israel. Holding CIPP/E, CIPP/US, CIPM, and FIP certifications, he founded Strand Alliance and the Israeli Data Protection Professionals Forum. Dan served on the Privacy Protection Public Council for eight years, advised on Bill No 13, and lectures at Tel Aviv University.



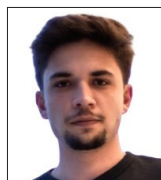
Eran Gandman is a partner at Or-Hof Law who advises technology companies on privacy, AI governance, IP, and corporate law. He guides clients through global frameworks like GDPR, CCPA, EU AI Act, DSA, and

more, developing compliance programs that balance legal rigour with business agility. He also manages Israeli corporate matters, including financing rounds and licensing agreements. Admitted to the Israeli Bar in 2021, Eran holds an LLB from Hebrew University and is certified as a CIPP/E and CIPM by the IAPP. He co-chairs the IAPP Tel Aviv KnowledgeNet Chapter, helping clients operate globally while maintaining practical operational compliance.



Netanel Aharon is an attorney specialising in privacy, data protection, and cybersecurity compliance. He began his legal career as an intern at Or-Hof Law and later rejoined the firm as an attorney.

Netanel supports clients navigating Israeli, European, and US privacy frameworks, including the GDPR, Israeli privacy laws and regulations, and US state and federal privacy laws, particularly within cross-border and multinational compliance projects in technology-driven environments. His work spans regulatory readiness, data governance, incident response, and implementation of privacy and cybersecurity programs. He also holds the CIPP/E certification, reflecting his expertise in the GDPR and European data protection standards.



Matan Adar is a legal intern at Or-Hof Law, working on technology law, data protection, and regulatory compliance matters. His practice focuses on advising technology-driven companies on privacy, data

governance, and complex regulatory frameworks, including cross-border compliance issues. During his legal training, he gained hands-on experience supporting tech companies with corporate and regulatory matters, combining legal analysis with practical, business-oriented solutions. He is developing expertise in corporate advisory, data protection, and emerging regulatory regimes.

Or-Hof Law

144 Begin Road
Midtown Tower, FL 21
Tel Aviv 6492102
Israel

Tel: +972 3562 0992
Fax: +972 3547 6515
Email: office@or-hof.com
Web: www.or-hof.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Regulatory Sources and Their Interaction

The Israeli privacy legal system is a tiered framework in which constitutional principles are implemented through statutes and regulatory guidance.

- Constitutional level: The Basic Law – Human Dignity and Liberty (1992) serves as the constitutional pillar. Section 7 protects the right to privacy and the confidentiality of communications and records. The courts rely on this right when interpreting the Privacy Protection Law, 5741-1981 (PPL), ensuring technological change does not erode substantive privacy protection.
- Primary statute: Following Amendment No 13 to the PPL (effective 14 August 2025), the PPL shifted from a technical database registration regime to a comprehensive personal data processing framework. Key developments include –
 - (a) updated definitions of “personal data” and “Data of Special Sensitivity”, aligned with international standards;
 - (b) mandatory appointment of data protection officers (DPOs) for public bodies and service providers to such data brokers, providers of direct mailing services, and organisations engaged in “systematic monitoring” or large-scale processing of Data of Special Sensitivity; and
 - (c) expanded enforcement powers for the Privacy Protection Authority (PPA), including administrative fines and binding suspension orders.

- Secondary legislation: Regulations enacted under the PPL, including –
 - (a) the Privacy Protection (Data Security) Regulations, 5777-2017 (the “Security Regulations”);
 - (b) the Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001 (the “Data Transfer Regulations”); and
 - (c) the Privacy Protection (Instructions for Data that was Transferred to Israel from the European Economic Area) Regulations, 5783-2023 (the “EEA-originated Data Regulations”).

Hierarchical Interaction and Sectoral Instruments

The Israeli legal system operates through a clear hierarchy.

- Constitutional level: this guides interpretation of all lower-level legislation.
- Primary legislation: the PPL operates as the *lex generalis* across sectors.
- Secondary legislation: regulations impose mandatory technical and organisational measures.
- Sectoral instruments: *lex specialis* rules apply, including health, financial, and labour law frameworks.

Israel retains EU adequacy status. The EEA-originated Data Regulations add a distinct layer of protection for EU-sourced data, including erasure and accuracy rights.

Extraterritorial Reach and Triggers

Unlike the GDPR’s explicit Article 3 triggers, extraterritorial application of the PPL is driven by case law and PPA interpretation. The PPA applies Israeli law where

processing of Israeli residents' data has a material privacy impact.

In summary, key application triggers include:

- targeting the Israeli market (eg, Hebrew interface, local marketing);
- databases containing significant volumes of Data of Special Sensitivity relating to Israelis; and
- processing activities conducted within Israel (such as by local servers or R&D centres).

Interplay With AI, Cyber, and Non-Personal Data

The PPL increasingly intersects with other specialised regimes.

- **AI:** Israel follows a sector-based approach. The 2025 PPA draft AI Guidelines (published 28 April 2025) apply the PPL across the AI life cycle, requiring privacy by design, transparency for automated decisions, and prohibiting unlawful scraping.
- **Cybersecurity:** The Israel National Cyber Directorate (INCD) manages national and critical infrastructure security, issues voluntary cyber guidelines, and handles cybersecurity incidents in Israel, often alongside the PPA for data breaches involving personal information.
- **Non-personal data:** The low “reasonable effort” re-identification threshold means that most datasets capable of re-identification are treated as personal data and are subject to the PPL. An anonymisation process applied to personal data would be regarded as a processing activity covered by the PPL, thereby subject to the supervision of the PPA.

1.2 Rights and Obligations

Processing of personal data under Israeli law is now governed by a strict “consent or authority” model, following Amendment No 13 to the PPL, bolstered by substantial administrative enforcement powers.

General Principles for Data Processing

The Israeli framework, particularly after Amendment No 13, is based on several core principles applicable to all organisations.

- **Informed consent:** Processing personal data without the data subject's informed consent constitutes

a violation of the law. Under current PPA guidance, consent must be granular and specific, and “bundled” consent (eg, service use combined with third-party marketing) is increasingly viewed as invalid.

- **Lawfulness of processing:** Processing personal data for purposes other than those lawfully established, or beyond the controller's authorisation, constitutes a violation of the PPL.
- **Purpose limitation:** Data collected for a specific purpose (eg, contract performance) may not be reused for a different purpose (eg, AI training) without new, separate consent.
- **Transparency and disclosure:** Section 11 of the PPL requires a “notice of collection” specifying –
 - (a) whether the provision of the data is legally required;
 - (b) the specific purposes of the collection;
 - (c) the identity of the controller;
 - (d) reasons for disclosing the identity of third-party data recipients;
 - (e) the consequences of refusal;
 - (f) the data subject's access and rectification rights; and
 - (g) the EEA-originated Data Regulations and PPA guidance on transparency and AI include additional disclosure requirements.
- **Proportionality and data minimisation:** Databases may contain only information that is strictly necessary for the declared purpose, and organisations must conduct periodic reviews to delete excess or outdated data.
- **Confidentiality:** Breach of confidentiality relating to personal data constitutes a serious criminal offence, punishable by up to five years' imprisonment.
- **Security:** The Security Regulations impose detailed, risk-based obligations on database owners and holders.

Data Subject Rights

Individual rights have expanded significantly, particularly for databases containing EEA-originating data not directly provided by the data subject.

- **Access:** Individuals may inspect personal data held about them, including digital records, audio-visual

materials, and assessment data used in recruitment.

- Right to rectification (correction) and a minimised deletion right: Incorrect, incomplete, or outdated data must be corrected or deleted upon request.
- Limited right to erasure: From 1 January 2025, individuals may request deletion of unlawfully obtained or no-longer-necessary EEA-originating data, subject to statutory exceptions.
- Opt out of direct marketing: Individuals have an absolute right to demand removal from direct mailing lists. Failure to comply can lead to an immediate administrative fine of ILS15,000 per violation.
- Withdrawal of consent: While not statutory, PPA draft guidance encourages controllers to respect consent-withdrawal requests.

Main Compliance “To Do’s” for Organisations

To mitigate exposure to the PPA’s enhanced enforcement powers, organisations should prioritise the following.

- Assess whether they need to appoint a DPO: This is required of public bodies and service providers to such public bodies, data brokers, providers of direct mailing services, and organisations engaged in “systematic monitoring” or large-scale processing of Data of Special Sensitivity.
- Data mapping: Maintaining up-to-date mapping of databases, systems, data categories, security levels, and EEA-originating data is required.
- Database definitions document: It is necessary to prepare and maintain a database definition document, which underpins Israeli data protection governance and compliance.
- Security compliance: Cybersecurity policies should be aligned with the Security Regulations, including non-standard requirements such as extended access-log retention.

1.3 Special Categories of Personal Data Definition

Amendment No 13 changed “sensitive data” to “Data of Special Sensitivity”. The Israeli definition is broader than the GDPR’s “Special Categories of Data”, covering political opinions, religious beliefs, medical and genetic data, sexual orientation, intimate family life, biometric identifiers, criminal records, personality

assessments, certain location data, payroll, financial transactions, and legally confidential data.

Enhanced Processing and Security Requirements

The PPL applies a unified consent model, coupled with heightened operational obligations.

- Consent: Under the 2025 PPA Guidelines, explicit consent is preferable, and it should also be informed, clear and accessible.
- Security tiers: Databases are classified as basic, medium or high security. Databases containing sensitive data fall under medium or high security, triggering enhanced safeguards such as security assessments and automated access monitoring.
- Mandatory appointment of a DPO: Organisations engaged in large-scale processing of Data of Special Sensitivity are required to appoint a DPO.

Processing Data of Minors

Israel does not have a standalone children’s privacy statute. Protection derives from multiple sources.

- Legal Capacity and Guardianship Law, 5712-1962: Minors lack full legal capacity; consent generally requires parental or guardian approval.
- PPA Guidelines on “Sharenting” and Social Media: These emphasise the best interests of the child, particularly in online exposure.
- Age assurance: Platforms targeting minors are expected to implement age-gating or age-assurance where sensitive profiling is involved.

Criminal Convictions and Foreclosures

Criminal data is tightly regulated by the Criminal Record and Rehabilitation of Offenders Law, 5779-2019, and the PPL. Private organisations cannot request or use this information, and the PPA bans unauthorised “blacklists” related to criminal history or foreclosures.

Sectoral Overlaps: Health and AI

Health data: This is subject to strict confidentiality, with PPA guidance requiring a Privacy Impact Assessment before deploying new digital health tools.

Artificial intelligence: Draft 2025 PPA guidance requires heightened transparency, explainability, and

human oversight when AI systems are trained on sensitive data.

1.4 Processing of Personal Data for Research and Development Purposes

Anonymisation of Patient Data for Product Development and Research

Under the Ministry of Health Circular 1/2018, companies serving Israeli healthcare providers can anonymise patient data for product development or research. This interim guidance sets out the framework until comprehensive regulation is established.

Key requirements

The circular favours anonymised data, requiring healthcare organisations to use it whenever possible. Identifiable patient data for secondary purposes is only accessible with legal authorisation or patient consent; otherwise, only anonymised data may be used.

Until unified standards exist, organisations should follow expert advice and best practices to ensure anonymisation is irreversible and re-identification is not possible.

Permitted uses

Anonymised data can support product development, quality improvement, research and statistics. Organisations must prove robust anonymisation and minimal re-identification risk.

Impact of European Health Data Space

As of early 2026, Israel's functional equivalent to the European Health Data Space (EHDS) is the Health Information Mobility Law, 5784-2024 (enacted July 2024).

Key similarities

The law reflects the EHDS "primary use" objectives by mandating health data portability between Health Maintenance Organisations (HMOs), hospitals and private clinics, via a centralised Ministry of Health system enabling real-time patient access management.

Main differences

- The Israeli framework currently excludes secondary use for research and innovation, which remains

governed by the Patient's Rights Law and Circular 1/2018.

- Most operational obligations will enter into force in July 2027, whereas EHDS implementation began in early 2025.
- Both regimes require high interoperability, with Israel adopting the Fast Healthcare Interoperability Resources (FHIR) standard to ensure compatibility with European systems.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

As of early 2026, Israel's regulatory framework for AI has matured significantly. While no single "AI Act" equivalent exists, the PPA and the Ministry of Innovation, Science and Technology have established a comprehensive regime through binding guidance and the full implementation of Amendment No 13. In addition, specific sectors have developed their own AI guidelines, notably, the Bank of Israel inter-ministerial team report addressing AI in the financial sector.

Primary Legal Framework and Specific Guidance

The use of personal data in AI is governed by the PPL, as amended by Amendment No 13, and supplemented by the draft 2025 PPA Guidelines on the application of the PPL to AI systems.

Key legal pillars include

- Applicability to the life cycle: Privacy obligations apply across all stages of AI use, including collection, training, deployment and inference.
- Inferred data: AI-generated conclusions (such as health or credit predictions) qualify as personal data and are subject to full protection.
- Scraping prohibited: Unauthorised scraping of personal data for AI training is prohibited, in the absence of a valid legal basis or explicit consent.

Risk-Based Regime and Automated Decision-Making

Israel follows a sectoral, risk-based approach rather than a horizontal framework:

- High-impact decisions – AI systems materially affecting individuals (eg, hiring, insurance pricing, or medical diagnosis) are treated with greater scrutiny.

- Sectoral overlays – Financial and life sciences regulators require explainability and bias testing.
- The “reasonableness” test – The courts apply administrative law principles to assess proportionality and non-discrimination in automated public-sector decisions.

Transparency and Data Governance

Under the 2025 PPA draft AI guidance, organisations are expected to:

- disclose AI use and provide meaningful explanations of data processing;
- conduct privacy impact assessments (PIAs); and
- involve boards of directors in approving AI governance, particularly where Data of Special Sensitivity is involved.

Human Oversight and Prohibited Categories

- Prohibited categories: While no categorical bans exist, practices such as social scoring are likely to be deemed unreasonable or unconstitutional.
- Human-in-the-loop: Strong preference exists for human review and appeal mechanisms in high-impact systems.

1.6 Data Breach Requirement

Israeli data breach notification requirements are governed by Section 11 of the Security Regulations and further detailed in PPA guidance dated 7 August 2022 (as amended 1 September 2025).

Notification Triggers and Assessment

Organisations must assess three elements when determining whether notification to the PPA is required:

- whether Israeli privacy law applies based on sufficient territorial connection;
- whether the incident constitutes a “Severe Security Incident”; and
- whether any statutory or regulatory exceptions apply.

Following notification, the PPA may instruct the organisation to notify affected data subjects.

Definition

A “Severe Security Incident” is defined by reference to the database’s security classification.

For high-security databases, any unauthorised use of data or damage to data integrity triggers notification.

For medium-security databases, notification is required where a substantial portion of the database is accessed without authorisation or its integrity is materially compromised.

Databases classified at the basic-security level are generally exempt from notification obligations.

Security Level Classification

Security classification is based on data sensitivity and database scale.

Medium security applies to databases containing Data of Special Sensitivity, databases used for direct marketing, and databases controlled by public bodies.

High security generally applies where medium-level databases grant access permissions to more than 100 individuals or contain records relating to 100,000 individuals or more.

Notification Procedures and Timing

Where notification is required, organisations must act immediately upon discovery. Notifications are submitted via the PPA’s designated online form and may be filed by legal representatives, including in English. Certain HR databases may qualify for exemptions and fall within the basic-security level.

Authority Investigations and Litigation Exposure

Following notification, the PPA may initiate investigations and order corrective measures, including mandatory notice to data subjects. Organisations face potential mass privacy litigation, as Israeli law provides civil remedies for privacy violations. This combined regulatory and litigation exposure heightens compliance and reputational risks, making early assessment and timely notification critical.

1.7 Regulators

The PPA, operating as an independent authority pursuant to Government Decision No 1890, serves as Israel's principal data protection regulator. Following the entry into force of Amendment No 13 to the PPL on 14 August 2025, the PPA has emerged as a highly active regulator with significantly expanded powers.

The PPA's mandate extends beyond classic data protection to encompass all privacy matters, including physical intrusions into privacy, and applies to both public bodies (including government ministries and municipalities) and private entities. It oversees compliance with the PPL and its implementing regulations, enforces regulatory guidance as binding obligations, and exercises authority over database registration and notification, data brokers, DPOs, and cross-border data transfers.

Investigative Workflow and Triggers

Enforcement proceedings may be initiated through multiple channels. Mandatory breach notifications trigger investigations in cases of Severe Security Incidents affecting medium or high-security databases.

In parallel, the PPA conducts proactive, cross-sector inspections, particularly in industries handling Data of Special Sensitivity. Media reports and public complaints increasingly prompt investigations, alongside routine audits of organisations processing large volumes of personal data.

Enforcement Powers

The PPA now wields extensive administrative powers. It may impose monetary sanctions reaching millions of shekels, issue orders suspending unlawful processing, initiate criminal investigations for serious violations, and mandate corrective measures, including notification to affected individuals.

Co-Ordination Mechanisms

Cross-border co-ordination is facilitated through Israel's EU adequacy status, requiring alignment with GDPR standards for databases containing EEA-originated data.

Binding Nature of Guidance

In practice, the PPA treats its directives as binding norms. PPA officials have stated that guidance will be enforced as if it were statutory, creating a quasi-legislative compliance layer beyond the text of the PPL and its regulations.

1.8 Enforcement Proceedings and Fines

Initiation and Conduct of Enforcement Proceedings

The PPA initiates enforcement proceedings through proactive and reactive channels. Proactive enforcement includes systematic monitoring, while reactive investigations are triggered by information from regulatory bodies, public institutions, media reports, complaints from individuals or competitors, and intelligence tools.

Once potential violations are identified, the PPA applies a graduated enforcement toolkit tailored to the severity and nature of the breach. Authorised investigators and supervisors may demand documents and information, enter premises where databases are reasonably believed to operate, conduct searches, and seize items pursuant to the Criminal Procedure Ordinance (Arrest and Search) [New Version], 5729-1969.

Computer investigations, particularly in residential premises, require prior judicial authorisation from a magistrate court's judge, and all PPA investigators are certified in computer investigations.

Available Sanctions and Remedies

The enforcement framework comprises criminal, administrative, and supervisory measures. Criminal investigations may lead to indictments. Administrative tools include supervised remediation, suspension or revocation of database registration, formal determinations of violations, and administrative fines for specific breaches of the PPL.

Administrative Fine Decision Process

After considering arguments submitted under Section 23 (kh) of the PPL, the PPA determines whether to impose an administrative fine and may reduce its amount. The authority must issue either a reasoned payment demand specifying the fine, payment period, and 45-day appeal right, or a reasoned decision

declining enforcement. If no arguments are submitted within the statutory period, the notice of intent automatically becomes a payment demand.

Enhanced Penalties for Continuing and Repeat Violations

For continuing violations, an additional 1% of the base fine accrues daily following issuance of a payment demand, excluding appeal periods unless otherwise ordered.

Repeat violations, defined as breaches of the same provision within two years of a prior fined violation, result in doubling of the penalty.

Reduced Fine Provisions

Administrative fines below statutory minimums may be imposed only in limited circumstances and subject to strict statutory conditions.

Appeal Rights and Timelines

Appeals against administrative enforcement actions must be filed with the magistrate's court within 45 days. Appeals do not automatically stay enforcement unless approved by the PPA director or ordered by the court. The courts may affirm, modify, annul, or remit the decision with instructions. Where a fine is paid and the appeal succeeds, the refund includes index-linked interest from payment to refund.

1.9 Enforcement Trends

Amendment No 13

The enactment of Amendment No 13 to the PPL in August 2025 represents the most significant reform of Israeli privacy law since 1981.

The amendment substantially expands the PPA's enforcement powers, including the authority to impose administrative fines, suspend database operations, and conduct criminal investigations.

It also introduced mandatory appointment of DPOs and enhanced transparency obligations, and it broadened the PPA's regulatory authority.

Adequacy Status Reaffirmation

In January 2024, the European Commission reaffirmed Israel's GDPR adequacy status, ensuring uninter-

rupted data flows between Israel and the EEA. While reinforcing Israel's attractiveness as a data hub, the decision maintains heightened compliance expectations for databases containing EEA-originated personal data.

Surge in Cyber-Related Enforcement

Following the October 2023 conflict, Israel experienced a rise in cyber-attacks. In response, the PPA intensified enforcement, managing 282 supervisory files and handling 224 Severe Security Incident reports in 2024. Enforcement actions included violation determinations and administrative fines against municipalities and medical centres for inadequate data security.

Cross-Sectoral Supervision Expansion

In 2024, the PPA expanded proactive, sector-wide audits across six additional industries, examining 175 entities in sectors including fintech, real estate, and mental health services. This supervision model, now embedded in Amendment No 13, aims to identify systemic risks at an early stage.

Practical Takeaways

Organisations should prepare for expanded DPO obligations, enhanced security testing (typically on an 18-month cycle), strengthened consent and transparency mechanisms, and continuous data mapping. Early enforcement actions, including an ILS70,000 fine imposed on HOT Telecommunication Systems Ltd, signal the PPA's intention to actively exercise its expanded powers.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Over the past 24 months, privacy and data-related litigation in Israel has increased markedly, with a rise in both individual claims and attempted class actions against private corporations and public bodies. Alongside regulatory enforcement by the PPA, courts are increasingly called upon to resolve civil disputes arising from data breaches and unauthorised processing of personal information.

Claimant Profiles and Causes of Action

Claims are brought by both individuals and groups. Individual actions typically arise in interpersonal and employment contexts, including unauthorised access to email or mobile devices, workplace surveillance, and unlawful disclosure of personal information. Such claims are commonly based on infringement of privacy without consent under section 2 of the PPL, together with negligence and breach of statutory duty.

At the collective level, there has been a growing number of class actions against technology companies, healthcare providers, and other data-intensive organisations. These cases generally concern large-scale data breaches or systematic unauthorised processing, and rely on privacy infringement, breach of confidentiality, unjust enrichment, and related tortious causes of action, including consumer misleading practices under the Consumer Protection Law, 5741-1981. Courts increasingly focus on admissibility issues, including standing and the applicability of consumer-based causes of action.

Remedies and Non-Material Damage

Israeli law expressly recognises compensation for non-material harm. Section 29A of the PPL permits statutory damages without proof of actual loss, subject to a statutory cap. Courts assess such damages on a case-by-case basis, considering the gravity of the infringement and deterrence needs, while generally adopting a restrained and proportionate approach. The Class Action Law 5766-2006 expressly permits compensation for non-monetary harm, reflecting the public interest in addressing widespread privacy violations.

2.2 Recent Case Law

Israeli courts have significantly clarified the procedural boundaries of privacy litigation following the enactment of Amendment No 13, particularly in class actions, which remain the primary vehicle for privacy claims in Israel.

Class Action Limits and the “Trader-Customer” Relationship

Recent case law reflects a restrictive interpretation of the Class Actions Law. In *Greenblat v Meta Platforms, Inc* (2025), the central district court rejected a

class action brought by non-users whose data was allegedly collected via third-party tracking, holding that commercial benefit alone does not establish a customer relationship. Similarly, in *Osher (Estate) v Tel Aviv Sourasky Medical Center* (2025), the court ruled that public hospitals generally provide public, rather than consumer, services, thereby limiting privacy-based class actions against public bodies.

The Modern Standard for Informed Consent

While narrowing standing, courts have raised the standard for consent. In *Aviv v Meta Platforms* (2025), the court approved a class action concerning the use of users’ names and profile photos in “social ads”. The court held that consent under Section 3 of the PPL must be genuinely informed, and that bundling consent to privacy practices within general terms of use is likely insufficient to establish lawful consent. This has driven a shift towards clear, separate and specific consent mechanisms.

Statutory Damages Without Proof of Harm

The courts have also reinforced Section 29A of the PPL, which permits statutory damages of up to ILS100,000 per violation without proof of actual harm. In *Ploni v Almonit* (2025), the court emphasised deterrence as the primary rationale, holding that unlawful technological intrusion alone may justify significant compensation, particularly where transparency obligations are breached.

2.3 Collective Redress Mechanisms

In Israel, collective redress is primarily pursued through class actions under the Class Actions Law. Although Israel lacks an equivalent to the EU Representative Actions Directive, its class action regime is highly active, particularly in consumer disputes, including privacy and cybersecurity claims.

Class Actions

Israel applies a “closed list” model, permitting class actions only for causes listed in the Second Schedule. In privacy and AI cases, claims are typically framed through consumer law, by characterising data processing as part of a service provided by a “trader” to a “consumer”.

Admissibility criteria and thresholds

A court may approve a class action if the following cumulative conditions are met at the preliminary stage.

- Personal cause of action: The representative plaintiff must demonstrate a direct claim; “non-user” classes have been rejected (*Greenblat v Meta*).
- Commonality: Substantial common legal or factual questions.
- Reasonable possibility of success: A prima facie merits assessment.
- Efficiency and fairness: The class action must be the most appropriate procedural vehicle.
- Adequacy of representation: Good faith and competent representation.

Procedure and indicative timelines

- Phase I – Certification: Typically decisive; respondents have 90 days to respond, and proceedings may last several years.
- Phase II – Merits: If certified, the case proceeds to trial, though most cases are settled or dismissed earlier.

Typical relief and statutory damages

Courts may award monetary compensation (individual or aggregate), statutory damages under Section 29A of the PPL without proof of harm, cy-près relief via the Class Actions Fund, and injunctive remedies.

Recent developments: privacy and AI contexts

Amendment No 13 strengthened privacy-based class actions, while recent case law confirms that web scraping alone does not establish a consumer relationship (*OpenAI v Haim Barak Cohen* (2025)). A proposed 2026 amendment seeks to curb abusive filings through pre-action notice mechanisms.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

As of 2026, regulation remains centred on the PPL, but emerging legislative initiatives increasingly address the broader data economy, drawing inspiration from the EU’s digital strategy.

Statutory Scope: The “Reasonable Identifiability” Test

The core principle remains that data is regulated under the PPL only if it relates to an “identified” or “reasonably identifiable” natural person.

- Anonymised data: Under the 2025 PPA Guidelines on Anonymization, data stripped of identifiers falls outside the PPL where re-identification would not be possible with reasonable effort, considering available technology and auxiliary datasets.
- Corporate and industrial data: Purely machine-generated data (eg, industrial telemetry) and internal business data are generally excluded from the PPL and are governed by the Trade Secrets Law, 5759-1999, and contractual arrangements.

Sectoral Data-Sharing Frameworks

Israel has no horizontal equivalent to the EU Data Act and data-sharing obligations are sector-specific:

- The financial sector (open banking) – The Financial Information Service Law, 5782-2021, mandates data sharing with licensed third parties at the user’s request, covering personal data and certain non-personal elements such as pricing and product metadata.
- The health sector (information mobility) – The Health Information Mobility Law, 5784-2024, facilitates data exchange between healthcare providers and standardises interoperability, including adoption of the FHIR standard.

The 2026 Digital and AI Reform: Towards a “Data Act”

A proposed 2026 reform package mirrors elements of the EU Data Act and AI Act, including:

- clarification of access and sharing rights in data generated by connected products;
- safeguards permitting refusal of data sharing where trade secrets are at risk; and
- cloud portability obligations aimed at reducing vendor lock-in.

Interaction With Cloud and IoT

Cloud and IoT regulation is shaped by PPA directives and IoT security guidelines. The framework distin-

guishes between controllers and holders, with cloud providers often acting as holders. Even non-personal cloud data is scrutinised where it forms part of mixed datasets containing personal data, triggering heightened safeguards under the EEA transfer regime.

3.2 Interaction of Data Regulation and Data Protection

The interaction between these frameworks has been clarified by Amendment No 13 and the 2025 PPA Guidelines. Data processing in Israel is now viewed as a continuous spectrum in which privacy, confidentiality and proprietary rights intersect.

Legal Basis and Purpose Limitation

The primary legal basis for processing personal data remains informed consent or statutory authorisation. Amendment No 13 has tightened the standard for a “lawfully established purpose”:

- Granular transparency – Under the 2025 PPA Guidelines, consent for complex processing (including AI training and IoT telemetry) must be explicit, separate from general terms, and assessed across the data life cycle.
- Purpose limitation – Section 8 (b) of the PPL strictly limits secondary use. In 2026, the PPA actively enforces this against “data creep”, particularly where consumer data is repurposed for AI development without renewed consent.

Statutory and Professional Confidentiality

Confidentiality obligations apply cumulatively, even where a lawful basis exists.

- Section 16 of the PPL: Prohibits disclosure of data obtained through one’s role or database access except for work purposes or by court order; breaches give rise to civil and potential criminal liability.
- Holder (processor) obligations: Cloud providers and other holders bear direct statutory duties, preventing reuse of client data unless expressly authorised and disclosed.

IP and Trade Secret Protection of Non-Personal Data

Purely non-personal data is protected primarily under trade secret and contract law.

- The “reasonable measures” test: Courts assess trade secret protection by reference to technical and organisational safeguards, increasingly aligned with the Security Regulations.
- Contractual protection: For IoT and life sciences datasets, contractual restrictions (such as no-scraping and no-derivation clauses) remain the principal IP protection mechanism.

The Interaction: the Identifiability Boundary

The key friction point arises where privacy obligations override IP interests.

- Reasonable effort: Data is treated as personal where re-identification is reasonably feasible.
- Regulatory consequence: Where proprietary datasets contain insufficiently anonymised Data of Special Sensitivity, the PPA may order deletion or “unlearning” of trained models, effectively negating the underlying IP.

3.3 Rights and Obligations Under Applicable Data Regulation

Following the full implementation of Amendment No 13 and the publication of multiple PPA Guidelines, Israeli data protection law has shifted from a technical registration-based regime to an accountability-driven framework.

The PPL now provides a comprehensive set of rights and obligations broadly aligned with international standards, while preserving distinct Israeli features and remaining materially different from a GDPR-style regime.

- Enhanced access and rectification: Data subjects have a statutory right to access their personal data and request correction of inaccurate or outdated information. Non-compliance may result in administrative fines and statutory damages without proof of harm.
- The right to deletion (erasure): Israeli law recognises a limited right to deletion. Deletion is mandatory

for direct marketing databases and for personal data transferred from the EEA other than by the data subject. In other cases, data must be deleted once the lawful purpose is exhausted; no general “right to be forgotten” exists.

- **Transparency and disclosure (section 11):** Before collection, organisations must provide a clear privacy notice identifying the controller, processing purposes, legal or contractual requirements, and consequences of refusal. Amendment No 13 strengthened enforcement of these obligations.
- **Mandatory DPO and accountability:** Public bodies, data brokers and organisations engaged in large-scale or systematic processing of sensitive data must appoint a DPO and maintain statutory compliance documents, including database definitions, structure documentation, and a written information security procedure.

Rights and Obligations for Non-Personal Data

Israel lacks a horizontal equivalent to the EU Data Act; regulation therefore relies on sectoral rules and contracts.

- **Portability and interoperability:** These apply only in regulated sectors, notably financial services (Financial Information Service Law, 2021) and health-care (Health Information Mobility Law, 2024), with phased implementation through 2027.
- **Switching and termination:** Outside regulated sectors, exit and data retention rights are governed primarily by contract, subject to trade secret protections.
- **IP and trade secrets:** Non-personal data is typically protected as a trade secret under the Commercial Torts Law (1999), subject to reasonable safeguards.

Main Necessary Action for Organisations

To align with the 2026 framework, organisations should prioritise:

- appointing a DPO and an information security officer, where required under the PPL, and consider voluntary appointment where thresholds are not met;
- data mapping and classification, particularly of Data of Special Sensitivity;

- updating data processing agreements (DPAs) with vendors and cloud providers, and managing the vendor risk life cycle, including pre-engagement reviews, periodic cybersecurity audits, and oversight;
- maintaining and updating statutory documents under the Security Regulations;
- adopting internal AI governance policies;
- updating privacy notices to clearly disclose AI use, automated decision-making, and marketing activities, including consequences of refusal;
- conducting cybersecurity risk assessments and audits in line with the Security Regulations; and
- establishing and testing a security incident and breach notification response plan.

3.4 Regulators and Enforcement

The enforcement of data protection and privacy in Israel is carried out by a co-ordinated network of authorities that has become increasingly integrated as of early 2026. The primary regulator, the PPA, now operates under a mandate significantly expanded by the 2025 reforms.

The PPA

The PPA is the lead authority enforcing the PPL. Following Amendment No 13, it has transitioned from a registry-based supervisor to a full enforcement agency. The PPA is authorised to impose administrative fines of up to ILS320,000 per cybersecurity violation and up to millions of shekels for database and personal data governance violations; issue binding processing suspension orders; order deletion of unlawful databases (subject to court approval); and conduct criminal investigations, including searches and seizures under partial judicial oversight.

The Israel Competition Authority (ICA)

The ICA enforces the Economic Competition Law and increasingly co-ordinates with the PPA where data concentration raises competition concerns. In 2025–2026, it scrutinised data-intensive mergers, particularly in the technology and fintech sectors. Co-ordination is formalised through inter-ministerial mechanisms, notably under the Financial Information Service Law, balancing data portability with privacy and security requirements.

The Israel National Cyber Directorate (INCD)

The INCD is responsible for national cybersecurity and critical infrastructure protection. While the PPA addresses privacy impacts, the INCD provides technical guidance and incident containment. Co-ordination is most visible during Severe Security Incidents, where reporting to both authorities may be required.

Sectoral Competent Authorities

Additional regulators enforce privacy-related obligations within their domains:

- The Bank of Israel – Banking privacy and open banking supervision.
- The Ministry of Health – Confidentiality and data sharing under the Patient Rights Law and the Health Information Mobility Law (2024).
- The Securities Authority – Disclosure of material privacy incidents by public companies.

Recent Enforcement Trends in 2026

Key trends include:

- lateral supervision – sector-wide audits focusing on systemic compliance;
- board level accountability – privacy-treated as a governance risk, with potential director exposure for compliance failures under PPA guidance;
- the AI enforcement drive – proactive action against unauthorised web scraping and biometric processing, supported by pre-rulings; and
- judicial barriers to digital searches – digital searches require narrowly tailored judicial authorisation to ensure proportionality.

4. Sectoral Topics

4.1 Use of Cookies

Following the entry into force of Amendment No 13 to the PPL, the 2025 PPA Guidelines on Informed Consent, the PPA's 2021 recommendation for cookie opt-in in its guidance on Privacy in Advanced Payment Methods, and the rise in cookie-related class actions, the Israeli market has placed increased focus on cookie consent. As a result, Israeli websites increasingly deploy cookie banners in various formats.

Status of Identifiers as Personal Data

Under the modernised PPL, personal data includes any information enabling identification with reasonable effort. This may include:

- online identifiers – cookies, MAC addresses, and advertising IDs (such as IDFA or AAID);
- network data – IP addresses and device fingerprints; and
- geolocation – real-time and historical location data collected via software development kits (SDKs).

As these identifiers may qualify as personal data, their collection requires an identifiability assessment and may trigger full PPL obligations, including notice and informed consent requirements.

The Mandatory Opt-In Consent Model

Although the PPL does not expressly regulate cookies, the 2025 PPA draft consent guidance requires informed, freely given consent for processing personal data, including common cookie-based activities such as analytics, advertising, user journey analysis, and marketing automation.

The following problem areas and solutions have been identified:

- Implied consent difficult to substantiate – The PPA indicates that reliance on implied consent requires substantial evidence of actual consent.
- Defective consent: Pre-ticked boxes and vague descriptions are considered invalid, with the burden on organisations to demonstrate valid consent.

Transparency and Notice Requirements (Section 11)

At the point of collection, users must receive notice identifying the controller, specifying processing purposes, explaining consequences of refusal, indicating access and rectification rights, and disclosing third-party recipients and purposes of data sharing.

4.2 Personalised Advertising and Other Online Marketing Practices

The regulation of personalised and targeted advertising in Israel is governed by a framework significantly modernised through Amendment No 13 to the PPL.

The Two Regulatory Pillars

Targeted advertising operates under two complementary statutes:

- The PPL – Governs profiling and direct mailing, defined as contacting individuals based on database segmentation.
- The Communications Law (Telecommunications and Broadcasting), 5742-1982 (the “Spam Law”) – Section 30A regulates the transmission of commercial messages via electronic means, including email and other electronic messages, mobile text messages, faxes and automated calls.

Profiling and Data of Special Sensitivity

Amendment No 13 expanded Data of Special Sensitivity to include location data, financial activity, and biometric identifiers.

Mandatory DPO

Entities whose core activity is to provide direct mailing services and which process the data of over 10,000 individuals must appoint a DPO.

Database registration

Registration remains mandatory for databases for the commercialisation of personal data, including data brokers and potentially, ad-tech companies.

Consent and Opt-In Requirements

Under the PPL, direct mailing notices must disclose the controller’s identity, data source (especially third-party data), opt-out rights and, where applicable, the database registration number. Under the PPA’s 2017 Direct Mailing Guidelines, consent for direct mailing services unrelated to the transaction’s purpose (eg, lead generation or data enrichment) must be obtained through an active and explicit indication of consent.

Following *Aviv v Meta Platforms* (2025), bundling consent to privacy practices, particularly advertising uses, with acceptance of general terms of use is likely to invalidate such consent.

By contrast, where an organisation sends direct mailing to its own customers regarding products or services related to its core offering, it is generally sufficient to disclose the intended use and provide an opt-out

mechanism, even if opting out results in service termination.

Under the Spam Law, prior written or electronic consent is required, subject only to the narrow “existing customer” exception. Consent to receive advertising must be separate from consent to terms of use or other privacy practices.

Protection of Children and Sensitive Categories

Children’s privacy (under 18)

Minors generally lack the legal capacity to consent independently. However, legal acts that minors of their age are accustomed to performing, such as routine, low-risk transactions, are generally valid. Platforms targeting children should implement age-assurance mechanisms, and profiling based on children’s sensitive data requires verified parental consent.

Sensitive profiling

Advertising based on Data of Special Sensitivity requires explicit opt-in. The PPA’s 2025 AI Guidance cautions against indirect “inference attacks” designed to deduce sensitive traits.

4.3 Employment Privacy Law

The landscape for workplace privacy in Israel is shaped by the PPL and its regulations, together with landmark rulings of the National Labor Tribunal and additional labour case law.

The Core Legal Standards

The main governing principles are as follows.

- In *Isakov v State of Israel* (2011) (“*Isakov*”), the National Labor Tribunal required any employer seeking access to an employee’s mailbox and digital assets on the employer’s computer systems to meet cumulative tests of legitimacy, proportionality, and transparency.
- In the *New General Federation of Labor (Histadrut) v the Municipality of Kalanswa* (2017), the National Labor Tribunal prohibited employers from requiring employees to use a fingerprint-based biometric attendance system without authorisation by law, or with the employees’ informed and freely given, separate and explicit consent.

- Under the Security Regulations, subject to certain conditions, databases containing employees' personal data are subject to a low level of security (the basic level), even though they contain Data of Special Sensitivity.
- Use of CCTV in the workplace environment is subject to substantial governance rules and limitations under the PPA Guideline 5/17.
- Use of location-based (eg, through GPS) monitoring of employees is restricted to necessary use cases and only during work time, pursuant to several Labor Tribunal decisions.
- Employers do not have access to employees' and job candidates' criminal records and are forbidden to take into consideration any criminal proceedings related to employees and job candidates, even if the information is received indirectly, including from media and online resources.

Monitoring and Time Tracking

Monitoring is permitted only for legitimate business purposes and with maximum transparency:

- Email and IT monitoring – Employers may monitor professional mailboxes only. Access to personal mailboxes requires a court order. Mixed mailboxes may be accessed only with employee consent and under strict limitations.
- Video surveillance – Under *Mark Friedman Ltd v Elkner* (2025) and PPA guidance, cameras near individual workstations are generally prohibited; surveillance is permitted only in common areas for security purposes and pursuant to a written policy.
- Biometric identification – As biometric data is highly sensitive, employers must provide non-biometric alternatives and may not disadvantage employees who refuse biometric identification.

Remote Work and IT Systems

The PPL contains no specific provisions on employee monitoring; the applicable framework is derived primarily from *Isakov* and PPA Guideline 5/17 (Use of Surveillance Cameras in the Workplace).

Monitoring of digital activity is considered a significant intrusion and is permitted only where it serves a defined and legitimate purpose, complies with pro-

portionality, is conducted under a clear policy, and is supported by informed consent.

In remote or hybrid work environments, monitoring must therefore be narrowly tailored, limited in scope and duration, and designed to minimise intrusion into employees' private content, whether employer systems or personal devices are used.

Background Checks and Recruitment

The processing of applicant data is governed by the PPL, the Equal Opportunities in Employment Law, 5748-1988, and the Criminal Information and Rehabilitation of Offenders Law, 5741-1981.

Employers are generally prohibited from requesting criminal record certificates, except where expressly authorised by law and strictly relevant to the position. Even then, processing remains subject to necessity, proportionality and purpose limitation.

PPA Guideline 2/2012 requires transparency regarding assessment methods, informed consent, proportional data collection, and deletion of applicant data once no longer required. These principles apply to assessment centres and technology-assisted recruitment tools to the extent personal data is processed.

4.4 Data Protection in M&A

The intersection of privacy law and M&A in Israel is governed by the modernised PPL, following Amendment No 13, and PPA Directive 2/2024 on the Transfer of Ownership in a Database.

Pre-Closing and Due Diligence

Any disclosure of personal data during due diligence is subject to strict proportionality:

- Data minimisation – Sellers should avoid sharing identifiable data (such as full employee files or unmasked customer lists). The PPA expects the use of clean rooms, and anonymised or aggregated datasets.
- Confidentiality agreements – Disclosures must be covered by NDAs containing dedicated data protection clauses, strictly limiting use to transaction evaluation.

- Risk assessment – Buyers should review the target's Database Definition Document and confirm whether a DPO was appointed where legally required.

Change of Control and Notification Requirements
PPA Directive 2/2024 treats database transfers as events affecting data subjects' rights:

- Mandatory notification – Data subjects must be informed of the change in ownership and the identity of the new controller, and allowed to exercise their rights, including deletion prior to transfer.
- Consent v notice – Where the new owner's characteristics differ substantially from those of the original owner in a manner likely to affect data subjects' rights or expectations, notice alone may be insufficient and prior consent may be required, even if processing purposes remain unchanged.

Circumstances Requiring Explicit Opt-In Consent
Explicit consent is required where there is a:

- change of purpose and the buyer intends secondary use beyond the original purpose (eg, AI training or cross-selling); and/or
- material difference in the nature of the owner, and the buyer's activities or ethical profile differ substantially from those of the seller.

Post-Closing Integration and Compliance

After closing, the buyer assumes full controller responsibility for:

- Database registration and notification – assessing whether notification or registration obligations are triggered.
- Updating governance documents – updating the Database Definition and Database Structure Documents and applying the buyer's security regime in accordance with the Security Regulations.
- Statutory liability – buyers may inherit liability for past violations. Enhanced privacy due diligence and contractual indemnities have therefore become standard in Israeli M&A transactions.

5. International Considerations

5.1 Restrictions on International Data Transfers

Legal Framework

Cross-border data transfers are governed by the Data Transfer Regulations and the PPL.

- Personal data: Regulation 1 prohibits transfers from Israel unless the destination ensures a level of protection no less than that provided under Israeli law.
- Non-personal data: This is generally outside the ambit of the PPL, though sectoral regimes (eg, banking, insurance, defence and export control) may restrict transfers of sensitive industrial or state-related data.

What Counts as a "Transfer"

The PPL and PPA guidelines do not define "transfer". However, as with the GDPR, it is likely that the interpretation of transfer will include:

- physical or digital relocation of data to foreign servers (eg, Cloud storage); and
- remote access.

Mechanisms for Lawful Transfer

Transfers are permitted where adequacy exists (Regulation 1) or an exemption applies (Regulation 2), including:

- the data subject having given informed consent for the transfer;
- transfer to a country that has ratified Convention 108;
- transfer to a country recognised as "adequate" by the EU Commission;
- contractual safeguards binding the recipient to Israeli-equivalent data protection standards;
- intra-group transfers to controlled affiliates (eg, subsidiaries) subject to guaranteed protections;
- vital interests, where the transfer is necessary for the data subject's health or physical well-being and consent cannot be obtained;
- public availability, where data was lawfully made public or opened for public inspection;

- public safety or security, where the transfer is necessary for such purposes; and
- mandatory transfers required under Israeli law.

Onward Transfers

Following the PPA's 2024–2025 position papers, Regulation 3 is applied more flexibly:

- controller consent – prior written approval required;
- equivalency – onward transfer must meet the same standards as a direct transfer from Israel; and
- sub-processing – sub-processors must be bound by equivalent obligations.

EEA-Originating Data

Under the EEA-originated Data Regulations, enhanced protections apply:

- expanded rights – stronger erasure, accuracy, and notice rights apply regardless of nationality; and
- purpose limitation – processing must strictly align with the original EEA transfer purpose.

5.2 Government Notifications and Approvals Export Control (Defence and Dual-Use)

Israel maintains a stringent export control regime under the Defence Export Control Law (2007) and the Import and Export Order (Dual-Use).

Scope of applicability

The Export Control Law and Export Order apply to:

- defence items – products, services, or know-how (including data) listed on the Defence Export Control List, based on the Wassenaar Arrangement and Israeli security needs;
- dual-use items – civilian goods with potential military application; and
- encryption – defence-grade encryption (Ministry of Defence) and civilian encryption products (Ministry of Economy).

Requirements and filings

- Registration with the Defence Export Control Agency (DECA/API).
- A marketing licence is required before negotiations or disclosure of technical data to foreign parties.

- An export licence is required for the actual transfer of goods or know-how.

Privacy and Data Protection

Cross-border transfers of personal data are regulated separately under the Data Transfer Regulations.

Scope of applicability

Any transfer of personal data from an Israeli database to a recipient outside Israel.

Requirements and filings

- Transfers of personal data do not require prior filing or approval from the PPA.
- Where database registration is required, the registration must disclose overseas data transfers.

5.3 Data Localisation Requirements

There is no general data localisation or residency requirement under Israeli law. Instead, the PPL and the Data Transfer Regulations regulate cross-border transfers rather than mandating domestic storage.

In practice, sector-specific regulation and the likely interpretation of what constitutes a “transfer” impose significant practical constraints.

Data Localisation and Remote Access Across Sectors

Sector-specific regimes govern data storage, security and access. Financial services, insurance and pensions, healthcare, and public bodies apply tailored rules reflecting confidentiality, risk, and national security concerns.

Organisations operating across sectors must therefore navigate overlapping and cumulative obligations.

Financial Sector Example

The financial sector demonstrates how functional localisation requirements arise in practice.

Directive 362 (Cloud Computing) restricts banking corporations from storing or processing sensitive information on foreign cloud infrastructure unless GDPR-equivalent protection is ensured.

Directive 364 (Management of IT, Information Security, and Cyber Protection Risks) permits remote access to sensitive systems only under strict safeguards, including encryption, multi-factor authentication, continuous monitoring, and access limited by business necessity.

In effect, while no formal localisation mandate exists, sectoral rules often produce localisation-like outcomes across regulated industries.

5.4 Blocking Statutes

Blocking Statutes and Foreign Judgments

Israel has no general “blocking statute” prohibiting compliance with foreign discovery. However, sector-specific secrecy regimes may effectively restrict disclosure.

- Foreign Judgments Enforcement Law, 5718-1958: Foreign judgments, including discovery orders, are not self-executing and require an Israeli court declaration of enforceability.
- The “Public Policy” Defence: Enforcement will be denied where it contradicts Israeli public policy, including disproportionate infringements of privacy or trade secrets.

Foreign Discovery and the Hague Evidence Convention

Israel is a party to the Hague Convention on the Taking of Evidence Abroad (1970).

- Procedure: Discovery is pursued through a letter of request, executed under Israeli court supervision.
- Restrictions: Disclosure is limited to specific, relevant documents; broad discovery and pre-trial depositions are generally prohibited.

Sanctions Compliance (the 2026 Shift)

Traditionally, Israeli private entities were not required to comply with non-UN foreign sanctions in the absence of a legal nexus.

A Bank of Israel Directive (January 2026) now requires banks to limit the accounts of people sanctioned by allied jurisdictions to support financial stability and correspondent banking.

Interaction with Privacy Law (Amendment No 13)

The PPL functions as a practical constraint on foreign disclosure.

- Legal obligation exception: Disclosure is permitted only where required under Israeli law; foreign subpoenas alone are insufficient.
- Purpose limitation: Data collected for service provision cannot be repurposed for foreign litigation without informed consent.
- Judicial balancing: The courts apply a proportionality test, weighing privacy rights against foreign judicial interests.

5.5 Recent Developments

The most significant recent change in Israel impacting the Data Transfer Regulations is Amendment No 13 to the PPL. The amendment gives the PPA greater enforcement powers, including the right to issue fines when organisations do not comply with orders to stop processing data in violation of Data Transfer Regulations. For example, ignoring a PPA order to halt unlawful data transfers can lead to significant penalties.

Since 1 January 2025, individuals have been able to request deletion of their personal data transferred from the EEA to Israel by third parties. This right also covers any other personal data in Israeli databases that contains EEA-originating data.



Law and Practice

Contributed by:

Paolo Balboni, Luca Bolognini, Nicolò Maria Salvi and Davide Baldini
ICT Legal Consulting

Contents

1. Legal and Regulatory Framework p.200

- 1.1 Overview of Data and Privacy-Related Laws p.200
- 1.2 Rights and Obligations p.200
- 1.3 Special Categories of Personal Data p.201
- 1.4 Processing of Personal Data for Research and Development Purposes p.203
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.203
- 1.6 Data Breach Requirement p.204
- 1.7 Regulators p.204
- 1.8 Enforcement Proceedings and Fines p.205
- 1.9 Enforcement Trends p.206

2. Privacy Litigation p.206

- 2.1 Privacy Litigation Overview p.206
- 2.2 Recent Case Law p.206
- 2.3 Collective Redress Mechanisms p.207

3. Requirements for the Protection and Processing of Non-Personal Data p.207

- 3.1 Objectives and Scope of Data Regulation p.207
- 3.2 Interaction of Data Regulation and Data Protection p.207
- 3.3 Rights and Obligations Under Applicable Data Regulation p.208
- 3.4 Regulators and Enforcement p.208

4. Sectoral Topics p.209

- 4.1 Use of Cookies p.209
- 4.2 Personalised Advertising and Other Online Marketing Practices p.209
- 4.3 Employment Privacy Law p.209
- 4.4 Data Protection in M&A p.210

5. International Considerations p.211

- 5.1 Restrictions on International Data Transfers p.211
- 5.2 Government Notifications and Approvals p.211
- 5.3 Data Localisation Requirements p.212
- 5.4 Blocking Statutes p.212
- 5.5 Recent Developments p.212

ICT Legal Consulting (ICTLC) is an international law firm that provides strategic legal and regulatory support across privacy, data protection, intellectual property, and technology, media and telecommunications (TMT) law, with a strong focus on the normative and operational aspects of cybersecurity. The firm assists organisations in designing and implementing governance, compliance and security frameworks that meet the highest international standards. With over 80 professionals and a network active in more than 65 juris-

dictions, ICTLC combines global co-ordination with local insight. Through its sister company **ICT Cyber Consulting**, the firm offers integrated cybersecurity services, including legal-technical risk assessments, resilience planning, and alignment with frameworks such as NIS2, DORA and the Cyber Resilience Act. ICTLC's multidisciplinary expertise enables clients to navigate complex digital regulations and strengthen trust, compliance and resilience across their global operations.

Authors



Paolo Balboni is a leading European ICT, privacy and cybersecurity lawyer, serving as the Data Protection Officer for multinational companies. Admitted to the Milan and Amsterdam Bars, he is founding partner of ICT Legal

Consulting and ICT Cyber Consulting. He advises on legal matters involving data protection, cybersecurity, AI, IoT, IT contracts and digital regulation. Paolo is a professor at Maastricht University, and holds positions with the EPO and European Commission expert groups. He is a published author and frequent keynote speaker. His expertise spans multiple sectors, and he has contributed to key EU regulatory frameworks, including the GDPR and cloud data protection codes.



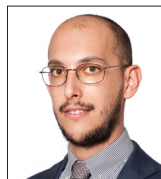
Luca Bolognini is a prominent privacy and data protection attorney, admitted to the Italian Supreme Court, and is founding partner of ICT Legal Consulting. He serves as President of the Italian Institute for

Privacy and Data Valorisation, co-founded several cybersecurity ventures, and directs Giuffrè Francis Lefebvre's "IUS Privacy Portal". Recognised internationally by Chambers Europe, Luca frequently contributes to European research initiatives, teaches at numerous prestigious universities, and actively publishes influential works addressing privacy, data protection, cybersecurity, artificial intelligence and digital innovation. His extensive scholarship emphasises balancing technological advancement with robust legal and ethical frameworks.



Nicolò Maria Salvi has been advising on personal data protection and ICT law since 2017, with a focus on data protection compliance and legal issues related to the use of new technologies. He is a partner at ICT

Legal Consulting, a certified Data Protection Officer and a certified auditor under the Europrivacy certification scheme. He holds a master's degree in Data Protection and Data Protection Design, and is enrolled in the Register of the Italian Institute for Privacy and Data Valorisation. He also serves as assistant professor in Constitutional and Media Law at LUISS Guido Carli University.



Davide Baldini is a lawyer and managing partner of ICT Legal Consulting. He advises multinational companies and innovative start-ups on data protection and IT contracts. He is a qualified Data Protection

Officer (ECPC-B) from Maastricht University, and a certified auditor for the Cloud Security Alliance Code of Conduct and the Europrivacy Certification Scheme. He is the author of several essays and articles for legal blogs and top-tier law journals. He is a PhD candidate in International and European Law at the University of Florence, where he is working on artificial intelligence and algorithmic discrimination.

ICT Legal Consulting

ICT Legal Consulting
Via Borgonuovo 12
20121 Milan
Italy

Tel: +39 0284 2471 94
Fax: +39 0270 0512 101
Email: info.legal@ictlc.com
Web: www.ictlegalconsulting.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Italian regulatory framework on the protection of personal data and privacy is dictated by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (GDPR). To the extent that such protection is not mentioned by the GDPR, it is regulated by Legislative Decree No 196/2003 (the “Privacy Code”).

Further detailed rules are contained in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as transposed into Italian law by the Privacy Code.

With reference to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, the regulatory framework is instead governed by EU Directive 2016/680, transposed into the Italian legal system through Legislative Decree No 51/2018. Finally, other specific indications and/or interpretations are contained in the decisions, recommendations and guidelines issued by the national supervisory authorities and the European Data Protection Board (eg, in Italy, the requirements for system administrators).

Concerning the extraterritoriality application, Article 2 of the GDPR addresses the application to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the EU; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.

Finally, as regards the interaction with artificial intelligence (AI) rules (Regulation (EU) 2024/1689 and Italian Law No 132/2025) and with cybersecurity rules (in particular, Italian Legislative Decree No 138/2024 transposing Directive (EU) 2022/2555, together with the determinations of the National Cybersecurity Agency in the NIS2 framework, Italian Law No 90/2024, and all implementing measures of Regulation (EU) 2022/2554), these instruments expressly defer to EU personal data protection law, leaving its content and scope unchanged and fully applicable.

1.2 Rights and Obligations

General Principles Relating to Processing of Personal Data

According to Article 5 (1) of the GDPR, personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
- collected for specified, explicit and legitimate purposes and not further processed in a manner

that is incompatible with those purposes (“purpose limitation”);

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
- accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (“accuracy”);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (“storage limitation”); and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).

In addition, the data controller shall be responsible for, and be able to demonstrate compliance with, such principles (“accountability”).

Lawfulness of Processing

Any processing of personal data must be based on at least one of the following legal bases provided for in Article 6 (1) of the GDPR:

- the data subject has freely given specific, informed and unambiguous consent to the processing of their personal data;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are

overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data (particularly where the data subject is a child) – in this case, the data controller is required to carry out an assessment of the legitimate interest pursued in relation to the rights and freedoms of the data subject by conducting a balancing activity that may possibly be challenged by the supervisory authority or the court.

Data Subjects' Rights

Data subjects have certain rights under the GDPR in order to allow them to have continuous and effective control over their personal data. In particular, data subjects have the right to:

- request access to their data (by receiving a copy of it) or to all information relating to the processing of their personal data (the purpose of processing, the recipients to whom the data is disclosed, any transfers outside the European Economic Area (EEA), etc);
- obtain the rectification of inaccurate or incomplete personal data;
- obtain the deletion of their personal data in the cases provided for in Article 17 of the GDPR;
- obtain the restriction of processing in the cases provided for in Article 18 of the GDPR;
- obtain their personal data in a structured and commonly used format or to request the transmission of such personal data to another data controller, where the legal basis of the processing is the consent of the data subject or the performance of a contract;
- object to processing based on legitimate interest or the performance of a task carried out in the public interest or in the exercise of official authority;
- not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the subject or similarly significantly affects them;
- withdraw the consent given; and
- lodge a complaint with a supervisory authority.

1.3 Special Categories of Personal Data

Special Categories of Personal Data

According to Article 9 of the GDPR, processing of personal data revealing racial or ethnic origin, politi-

cal opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, is prohibited except in the following cases:

- where the data subject has given explicit consent to the processing of that personal data for one or more specified purposes;
- where processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection law in so far as it is authorised by the law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- where processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- where processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim, and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and that the personal data is not disclosed outside that body without the consent of the data subjects;
- where processing relates to personal data that is manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- where processing is necessary for reasons of substantial public interest, on the basis of the law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- where processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employ-

ee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of the law or pursuant to contract with a health professional;

- where processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of the law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject – in particular, professional secrecy (in this specific regard, reference is made to Article 2-sexies of the Privacy Code); and
- where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

According to Article 2-septies of the Privacy Code, the Italian supervisory authority (*Garante per la Protezione dei Dati Personali* GDPR) may also specify particular safeguards for processing genetic data, biometric data and data concerning health.

Personal Data Relating to Criminal Convictions and Offences

According to Articles 10 of the GDPR and 2-octies of the Privacy Code – as amended by Article 71 (1)(g) of Law No 182/2025 – processing of personal data relating to criminal convictions and offences or related security measures is carried out only under the control of official authority or when the processing is authorised by the law providing for appropriate safeguards for the rights and freedoms of data subjects.

Data Relating to Minors

In accordance with Article 8 of the GDPR and Article 2-quinques of the Privacy Code, restrictions on the processing of minors' data concern their consent. In particular, minors who have reached the age of 14 may consent to the processing of their personal data in relation to the direct offer of information society services (below this age, consent must be given by those exercising parental responsibility). However, the data controller must draft the information and communications relating to the processing in particularly

clear and simple, concise and comprehensive language that is easily accessible and understandable to the minor.

1.4 Processing of Personal Data for Research and Development Purposes

Life sciences or medtech companies can anonymise patient data for product development or scientific research only if the outcome is true anonymisation in the GDPR sense. That means that the data must be rendered irreversibly non-identifiable, taking into account all means reasonably likely to be used for re-identification. In healthcare, this is a high bar, as clinical datasets are rich and easily linkable; the GPDP's approach is consistently strict, so mere removal of direct identifiers or standard pseudonymisation is not enough. If the company achieves genuine anonymisation, the dataset falls outside the GDPR and can be used for research and development without a GDPR legal basis.

Where full anonymisation is not realistically achievable, data remains personal (even if pseudonymised). Then, the company must rely on a GDPR Article 6 lawful basis and an Article 9 (2) condition for health data, most often the scientific research ground combined with Article 89 safeguards. The Italian Privacy Code rules on research (including the updated Article 110) support this pathway by allowing certain research uses with enhanced safeguards when informing individuals is impossible or disproportionate, but they do not remove the need for a lawful basis and accountability.

The Code of Conduct for management software developers approved by the GPDP in October 2024 reinforces this compliance logic for software/tech vendors working with hospitals: it operationalises privacy-by-design/default, clarifies that vendors typically act as processors for installation/maintenance/support, and expects robust security and life cycle controls. In practice, it pushes medtech vendors to ensure that any re-use/anonymisation for R&D is clearly covered contractually with the healthcare provider and supported by appropriate technical measures.

Looking forwards, the European Health Data Space Regulation (EU) 2025/327 (EHDS) is a major change

for these companies. It entered into force on 26 March 2025 and will apply in phases from 26 March 2027, with the secondary use regime (research/innovation/AI training, etc) becoming operational from 26 March 2029 and some data categories being phased in later. The EHDS will create a harmonised, permit-based route to access large volumes of electronic health data across the EU through national Health Data Access Bodies, typically in secure environments and often in anonymised/pseudonymised form. For life sciences and medtech firms, this should increase lawful access and legal certainty for research and development, but only under tighter governance, interoperability, auditability and anti-reidentification constraints.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

With regard to the use of AI systems, it is essential to note that both EU (AI Act) and national legislation refer to the GDPR and the Privacy Code for the regulation of personal data protection profiles relating to the use of AI tools. In this context, the first thing to note is the transparency obligations, as Articles 13 and 14 of the GDPR require data subjects to be provided with information on the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

In addition, Article 22 of the GDPR states that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, except where the decision is:

- necessary for entering into, or the performance of, a contract between the data subject and a data controller;
- authorised by the law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- based on the data subject's explicit consent.

In these cases, the data controller shall implement suitable measures to safeguard the data subject's

rights and freedoms and legitimate interests – at least the right to obtain human intervention on the part of the controller – to express their point of view and to contest the decision.

Lastly, it is likely that an AI tool is also subject to the Data Protection Impact Assessment requirement under Article 35 of the GDPR.

1.6 Data Breach Requirement

In the case of a personal data breach, the data controller shall, without undue delay and where feasible no later than 72 hours after having become aware of it, notify the personal data breach to the GPDP, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Such notification should at least:

- describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach; and
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where the notification to the authority is not made within 72 hours, it shall be accompanied by reasons for the delay. In addition, where and in so far as it is not possible to provide all the information at the same time, the information may be provided in phases without undue further delay.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in addition to the notification described above, the data controller shall also communicate the personal data breach to the data subject without undue delay, describing in clear and plain language the nature of the personal data breach and the same above-men-

tioned information. Such communication to the data subject shall not be required if:

- the controller implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach – in particular, those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; and
- it would involve disproportionate effort – in such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Lastly, the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

1.7 Regulators

Supervisory authorities have limited regulatory power, mainly through the adoption of guidelines and opinions interpreting legal provisions. However, supervisory authorities (in Italy, the GPDP) also have supervisory powers to monitor compliance with data protection legislation, and benefit from investigative powers that include, *ex multis*, the possibility of requesting information from data controllers and data processors or conducting on-site checks and inspections.

In this context, the supervisory authority may request access to the documentation adopted (privacy policy, consents, internal policies and procedures, records of processing activities, etc) and to systems and databases. The GPDP's inspections may be triggered by the authority itself (based on an inspection plan adopted and published every six months, or following notification of a personal data breach) or by data subjects or other third parties (in the case of complaints or reports). Any decisions that are eventually adopted are published.

Data protection legislation may also be applied by the courts in the case of appeals lodged by individu-

als (particularly in the case of claims for damages or appeals against decisions of the supervisory authority).

1.8 Enforcement Proceedings and Fines

As mentioned in 1.7 **Regulators**, GPDP inspections may be triggered by the authority itself (on the basis of an inspection plan adopted and published every six months, or following the notification of a personal data breach) or by data subjects or other third parties (in the case of complaints or reports).

Preliminary Investigation

In the event of a complaint by a data subject, the GPDP shall verify the correctness and completeness of the complaint and, if necessary, grant the complainant a period of time to amend it, normally not exceeding 15 days. In the event of a correct and complete complaint (or in the event of an investigation on its own accord, such as following the notification of a personal data breach), the GPDP shall start a preliminary investigation, during which the documentation received is examined and/or further information is requested from the data controller or data processor.

In that scenario, inspections may also be carried out, during which the entity subject to inspection may be assisted by its trusted advisers and reserve the right to produce the documentation that is not immediately available within a reasonable period (as a rule, not exceeding 30 days). A record of the activity carried out shall also be drawn up, with particular reference to the statements made and the documents acquired, and a copy shall be given to the subject under inspection.

Closing of the Preliminary Investigation and Archiving

At the end of the preliminary investigation, the competent department within the GPDP may conclude its examination of the complaint by archiving it, when:

- the issue examined does not appear to be related to the protection of personal data or the tasks entrusted to the GPDP;
- there is no evidence of a breach of the relevant data protection regulations;

- the claim set out in the complaint is excessive, due in particular to its specious or repetitive character; or
- the issue raised by the complaint has already been examined by the GPDP.

In the case of a complaint, feedback is provided to the applicant, briefly stating the reasons why no action is being taken.

Initiation of Proceedings

If the matter is not dismissed following the preliminary investigation, the competent department shall initiate proceedings for the adoption of measures by the board of the GPDP, by means of its own communication to the data controller and/or data processor. The communication shall contain:

- a concise description of the facts and alleged breaches of the relevant data protection rules, as well as the relevant sanctioning provisions;
- an indication of the competent organisational unit where a copy of the investigative documents may be inspected and extracted; and
- the indication that, within 30 days of receipt of the notice, it is possible to send the GPDP defence papers or documents, and to ask to be heard by the GPDP.

Right of Defence

The addressee of the notice may exercise the right of defence by submitting written statements and documents within 30 days from the date of notification of the communication, as well as a personal testimony regarding the facts of the notice, where requested.

The addressee of the notice may request a short extension by specifically and duly motivating the request. The extension shall normally not exceed 15 days, and may be granted according to proportionality criteria and criteria relating to the operational/dimensional characteristics of the addressees themselves and to the complexity of the matter under examination. The addressee of the notice may also request a hearing before the GPDP.

Failure to submit written counterarguments or a request for a hearing shall not prejudice the continuation of the proceedings.

Decision

Where necessary, the board of the GPDP, by its own resolution, shall adopt the corrective and sanctioning measures referred to in Article 58 (2) of the GDPR (in the case of an administrative pecuniary sanction, the quantum is calculated on the basis of the criteria indicated by Article 83 of the GDPR). The decision is notified to the parties by the department, service or other organisational unit that has supervised the preliminary investigation.

Appeal Against Measures of the GPDP

Under penalty of inadmissibility, an appeal against the measures adopted by the GPDP must be lodged within 30 days from the date of communication of the decision or within 60 days if the appellant resides abroad, with the ordinary court of the place where the data controller resides, or with the court of the place of residence of the data subject. At the time of the appeal, it is also possible to request the court to suspend the enforceability of the contested decision.

The so-called “work ritual” applies to the judicial procedure, and the sentence that defines the judgment is not appealable before the judge and may prescribe the necessary measures and compensation for damages.

1.9 Enforcement Trends

Over the past 24 months, Italian enforcement has concentrated on a few high-risk clusters:

- telemarketing and unlawful lead chains, with record-level fines (notably the *Enel Energia* case) for weak control over data sources and processors;
- generative AI and web-scraping, where the GPDP has moved from warnings to major sanctions (eg, OpenAI/ChatGPT, Replika) focusing on lawful basis for training, transparency and child protection;
- biometrics/facial recognition, treated as exceptional and stopped when safeguards or voluntariness are insufficient;
- workplace monitoring via metadata and logs, now enforced as strictly as traditional surveillance; and

- cookies/dark-pattern consent, seen as basic compliance hygiene.

A parallel trend is the growing privacy-competition convergence, with Italian Competition Authority (AGCM) scrutiny on consent and data-combination practices.

2. Privacy Litigation

2.1 Privacy Litigation Overview

In recent years, data protection litigation in Italy has experienced significant growth, driven by an increasing awareness of rights among data subjects.

The most frequent disputes involve unlawful data processing, data breaches, and the improper use of personal data by companies and public administrations. Claims for compensation for privacy violations, particularly for non-material damages, are also on the rise.

In this context, the GPDP is playing a crucial role, imposing substantial fines that influence corporate strategies, seeking to stay ahead of other European authorities, and positioning itself as a leader on issues related to AI (for instance, the proceedings initiated against OpenAI and ChatGPT, which concluded with a sanction in December 2024) and employee monitoring, especially concerning the retention of metadata generated through employees’ use of email tools (ie, the decision against Regione Lombardia on metadata and logs relating to internet browsing).

2.2 Recent Case Law

The most significant recent decision for EU/Italian privacy litigation is the CJEU’s *Deloitte* judgment C-413/23 P (*EDPS v SRB*), 4 September 2025. The Court held that pseudonymised data is not automatically “personal data” for every actor: for a third-party recipient, the qualification depends on whether that recipient has reasonably likely and practically available means to re-identify individuals. If, in the recipient’s hands, identification is not realistically possible, the data may be treated as anonymous for that recipient, even though it remains personal data for the original controller who retains the re-identification key. The

Court set aside the General Court's approach because it had relied on an abstract presumption (pseudonymisation = personal data) without assessing Deloitte's concrete re-identification capability.

2.3 Collective Redress Mechanisms

The national legislation on personal data protection does not currently provide explicit regulation for collective redress mechanisms. However, data subjects may rely on the tools generally available under civil procedure law or those designed to protect their rights as consumers.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

In Italy, the protection and governance of non-personal data is largely shaped by directly applicable EU regulations, rather than by autonomous national legislation. There is no standalone Italian "horizontal" law equivalent to the EU Data Act; instead, Italy relies on the EU data strategy instruments, complemented only by sectoral or administrative measures.

The starting point is the Free Flow of Non-Personal Data Regulation (Regulation (EU) 2018/1807), which establishes the principle of the free movement of non-personal data within the EU. It prohibits unjustified data-localisation requirements imposed by member states, and promotes portability and switching for professional users of data processing and cloud services. Importantly, for mixed datasets (where personal and non-personal data are intertwined), the Regulation operates alongside the GDPR: the GDPR applies to the personal component, while the free-flow rules apply to the non-personal component.

This baseline is expanded by the Data Governance Act (Regulation (EU) 2022/868), which provides a cross-sector EU framework to increase data availability and sharing, covering both personal and non-personal data. It regulates the re-use of certain protected data held by public sector bodies, introduces trusted roles such as data intermediation service providers, and supports voluntary mechanisms such as data altruism and the development of Common European

Data Spaces. Italy has adopted implementing measures mainly to designate competent authorities and procedural arrangements, but the substantive regime remains EU-based.

Finally, the EU Data Act (Regulation (EU) 2023/2854) – applicable across the EU, including Italy, from 12 September 2025 – constitutes the central horizontal regime for access to and use of data generated by connected products and related services (ie, IoT ecosystems). It sets out rights and obligations for key actors such as data holders, users (B2C/B2B) and data recipients, and applies to both personal and non-personal data depending on the nature of the dataset, subject to GDPR compliance for any personal elements. A core pillar is the mandatory B2B/B2C data access and sharing framework, often under FRAND (fair, reasonable and non-discriminatory) terms, and another pillar addresses the cloud and edge layer by imposing rules on switching, interoperability and the removal of contractual/technical lock-ins in data processing services.

Beyond these EU Regulations, Italy has not enacted a separate Data Act-like statute. National activity is mainly confined to sector-specific governance (especially for public-administration data and cloud security classifications) and to procedural implementation where EU Acts require member state designation of authorities or enforcement structures.

3.2 Interaction of Data Regulation and Data Protection

These frameworks are designed to complement, not override, privacy and IP rules, so the interaction works in layers. When the data to be accessed or shared includes personal data (or is part of a mixed dataset), the GDPR remains fully controlling. The Data Act and the Data Governance Act do not create a new lawful basis on their own: any disclosure must still rely on an Article 6 GDPR ground already applicable to the data holder, and must respect all GDPR principles, including confidentiality, minimisation, purpose limitation, transparency and security. In practice, the user's Data Act access right can be exercised only within what is lawful under the GDPR, and any recipient of personal data must comply with the GDPR as an autonomous controller or processor.

For non-personal data, access and sharing obligations under the Data Act/Data Governance Act are balanced against IP rights and trade secret protection. The general rule is that sharing goes ahead, but the data holder may and should impose proportionate safeguards – for example, confidentiality clauses, technical access controls, or limiting the dataset to what is strictly necessary – so that disclosure does not destroy trade secret value or infringe IP. A refusal to share is allowed only in exceptional cases where no reasonable protective measures could prevent a serious risk of economic harm.

Thus, conceptually, the system is a “dual compliance gate”: the GDPR determines whether and how personal data can move; trade secret/IP law determines under what protections sensitive non-personal data can be shared, with access remaining the default outcome.

3.3 Rights and Obligations Under Applicable Data Regulation

As a baseline, the Free Flow Regulation guarantees that non-personal data can be stored and processed anywhere in the EU, banning unjustified localisation rules. It also promotes portability and switching for professional cloud users, mainly through industry codes of conduct, and confirms that mixed datasets are governed jointly by the GDPR (personal layer) and free-flow rules (non-personal layer).

The Data Governance Act does not impose broad private-sector access duties but sets trusted conditions for sharing. It regulates the re-use of certain protected public-sector data, creates a compliance regime for neutral data intermediation services, and enables voluntary “data altruism” channels.

The Data Act is the core horizontal regime. It gives users of connected products and related services a right to access the data they generate, and to require the data holder to share those data with a third party (data recipient). Data holders must design products/services so that data is accessible by default, and must share B2B data under FRAND terms, with additional safeguards for SMEs and controls on unfair contractual clauses. In parallel, the Act imposes strong switching, portability, interoperability and termina-

tion duties on providers of data processing services (cloud/edge), including removal of technical/contractual lock-ins and limits on switching/egress fees. Any flow involving personal data remains fully subject to GDPR requirements; the Data Act does not override them.

For organisations, the main action items are practical and contractual:

- map and classify product-generated data (non-personal/personal/mixed);
- build technical interfaces and APIs for user access and third-party sharing;
- update notices and B2B templates to reflect FRAND pricing and Data Act unfair terms rules;
- implement procedures to protect trade secrets proportionately when access is requested; and
- for cloud providers, revise pricing, contracts and architectures to enable effective switching and interoperable portability.

3.4 Regulators and Enforcement

In Italy, enforcement of the EU non-personal data regime is shared among multiple authorities. AgID is the lead authority for the Data Governance Act, overseeing data intermediation services, data altruism registrations, and public sector data re-use; it also functions as the co-ordination hub. When data sharing involves personal or mixed datasets, AgID works with the GPDP to ensure GDPR compliance. Where access or FRAND terms create competition or unfair-contract concerns, the AGCM intervenes, and the ACN provides support in cybersecurity/cloud-security aspects.

For the Data Act, Italy is moving towards a multi-authority model: digital/data-governance functions close to AgID, technical/market-surveillance authorities for connected products, the GPDP for the personal data layer, and the AGCM for FRAND, unfair terms and anti-lock-in issues. The main trend is co-ordinated enforcement: Data Act cases are increasingly treated as “hybrid” matters requiring simultaneous privacy, competition and technical oversight, with regulators prioritising practical outcomes (IoT user access and cloud switching) over purely formal classifications.

4. Sectoral Topics

4.1 Use of Cookies

In Italy, the general rule is set out by Article 122 of the Privacy Code (which transposes Directive 2002/58/EC), under which all cookies – and other similar tracking tools – other than those strictly necessary for the functioning of the website may be installed on the users' devices only with their consent.

In this regard, as clarified by the Guidelines adopted by the Italian Supervisory Authority in 2021, it is essential that consent for the use of cookies is collected in compliance with the principles established by the GDPR. Accordingly, it must be preceded by a multi-layered notice (cookie banner) that provides information about the cookies and the related personal data processing, and that allows the user to freely accept or refuse the use of cookies as well as to change their decision at any time.

A specific consideration applies to analytical cookies, which may be treated as necessary cookies (and therefore not require consent) only when:

- IP anonymisation features are enabled;
- the use of analytical cookies is strictly limited to the production of aggregated statistics; and
- they are used solely in connection with a single website or mobile application, such that they do not allow the tracking of users' navigation across different websites or applications.

4.2 Personalised Advertising and Other Online Marketing Practices

In Italy, the general rule is set out by Article 130 (1;2) of the Privacy Code (which transposes Directive 2002/58/EC), under which commercial and promotional communications by email, fax, telephone and similar means of communication require the prior consent of the user (natural or legal person). However, Article 130 (4) provides for an exception to the requirement of consent, allowing for the processing of the email address provided by the data subject in the context of the sale of a product or a service for the purpose of sending commercial communications aimed at the direct sale of products or services similar to those already purchased, provided that the data

subject has been adequately informed and does not refuse such use, either initially or on the occasion of subsequent communications.

With specific regard to telephone marketing activities, Article 130 (3-bis) provides that data controllers may lawfully contact all users who have not objected to receiving commercial communications by telephone by registering in the Register of Opposition. In this sense, pursuant to Law No 5/2018, users may enlist in the register in order to prevent subsequent communications and, at the same time, withdraw any consent previously given to the processing of their personal data for telephone marketing purposes. In fact, the data controller who intends to carry out telemarketing activities is required to consult the register at least every 15 days or, in any event, before the start of a new campaign.

On the other hand, online marketing may consist primarily of an activity carried out through the use of profiling and advertising cookies (see 4.1 Use of Cookies), or of behavioural advertising and targeting activities carried out through the use of external databases (especially those of social networks). In this second case, the jurisprudence of the CJEU and the interpretation provided by the European Data Protection Board (EDPB) in Guidelines 8/2020 clarify the need to carry out the activity on the basis of the prior consent of the data subject and, as a general rule, to reconstruct the privacy roles between the company and the social network as joint controllers of the processing to be regulated under Article 26 of the GDPR.

4.3 Employment Privacy Law

Processing carried out in the employment context is one of the sectors to which the GDPR defers to its regulation under national law, without prejudice to certain common guidelines and orientations first shared by WP29 and then by the EDPB, specifically regarding the vulnerable position of the data subject employee vis-à-vis the data controller employer (a situation that results in the presumption of the invalidity of any consents requested from the employee due to a lack of freedom).

Managing the Selection Process and the Employment Relationship

In these phases, the employer's activities must respect – more than ever – the principle of minimisation, ensuring that only personal data that is essential for the performance of work duties and that, to a large extent, is governed by labour law provisions (eg, Article 8 of Law No 300/1970 or Legislative Decree No 81/2008) is requested from the candidate or employee.

Remote Monitoring of Workers

Without prejudice to a general prohibition on the use of instruments (also based on AI) to monitor employee activities, this case is governed by Article 4 of Law No 300/1970, which legitimises the use of such tools solely for organisational purposes and the protection of company assets (eg, cybersecurity purposes). In this case, without prejudice to instruments that are essential and prearranged for the performance of work duties, the use of instruments for remote monitoring is permitted only if doing so is:

- agreed with the trade union representatives present in the company; or
- authorised by the competent Labour Inspectorate in the absence of trade union representatives in the company or in the event of there being no agreement.

In these cases, the employee data subject will have to be provided with additional and detailed information on what is normally provided for under Articles 13 and 14 of the GDPR; this can be done by adopting an internal regulation on the use of IT tools, for example, which also informs employees of the possible controls and their purposes.

However, although the agreement with trade union representatives or administrative authorisation is sufficient to legitimise the activity from the point of view of labour law, this does not exempt the employer from complying with the principles on the protection of personal data (eg, the principle of minimisation). In this sense, unencrypted or clear monitoring of the URLs surfed by employees is unlawful because, in terms of security purposes, the same results can be achieved by implementing filters that inhibit the surfing of potentially risky websites. On this point, see also the

Guidelines adopted by the GPDP on 1 March 2007 or the Guidelines on the metadata collected through the use of email accounts.

Whistle-Blowing and the Transparency Decree

The national legislation on whistle-blowing was updated to transpose Directive (EU) 2019/1937 through Legislative Decree No 2023/24, which made discipline uniform between the private and public sectors. With regard to the protection of personal data, the general principles dictated by the GDPR remain valid, concerning the obligations to set up reporting and management processes in compliance with the principles of privacy by default and by design, and with the need to ensure the confidentiality of the reporter (resulting in the inadequacy, for instance, of the email channel), carry out a Data Protection Impact Assessment (DPIA) on the processing, train and instruct the people who access the data and manage the reports, etc.

Further obligations (mainly informative) are also imposed by Legislative Decree No 104/2022 (the so-called “Transparency Decree”), which prescribes the need to carry out a DPIA and to provide additional information to data subjects in the event of “the use of automated decision-making or monitoring systems designed to provide indications relevant to the recruitment or assignment, management or termination of the employment relationship, the assignment of tasks or duties, as well as indications affecting the monitoring, assessment, performance and fulfilment of contractual obligations of workers”.

4.4 Data Protection in M&A

The value of personal data and consent databases as a corporate asset is often underestimated in corporate transactions. In this context, with regards to the sector in question, the main activity may consist of verifying the lawfulness and correctness of the processing of personal data that makes up a company's databases; this can be done by verifying the correctness and completeness of the information that the data controller had to provide to the data subjects pursuant to Articles 13 and 14 of the GDPR, and by examining the evidence of compliance with this information notice obligation.

Furthermore, where the processing of personal data is based on consent (eg, in the case of processing for promotional purposes or in the context of scientific research), it is essential to verify the correctness and ability to prove the consents collected from the data subjects and the effective capacity of the systems to receive any requests for withdrawal and/or opposition.

Following the M&A transaction, it is also essential that data subjects receive a communication informing them of the change in the identity of the data controller, as well as any other changes relating to the processing of personal data (new contact channels for the data controller and the Data Protection Officer, new methods for exercising rights, any transfer of data to third countries, etc). This communication should be provided upon first contact with the data subject or within 30 days.

5. International Considerations

5.1 Restrictions on International Data Transfers

European data protection legislation requires that any transfer of personal data that is undergoing processing or is intended for processing after transfer to a third country or to an international organisation (including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation) shall take place only if the level of protection of natural persons guaranteed by the GDPR is not undermined.

This therefore requires an examination of the legal provisions applicable to the third country or international organisation in order to understand the actual level of protection of personal data, taking into account the elements specified in Article 45 (2) of the GDPR. This analysis is carried out by the European Commission when it adopts the adequacy decisions referred to in Article 45 of the GDPR (decisions legitimising the transfer of personal data to the country or organisation benefiting from it).

In the absence of an adequacy decision, as clarified by the CJEU in its judgment of 16 July 2020 (the *Schrems II* judgment), this assessment is instead the

responsibility of the data controller or data processor who is intending to export the personal data. In such a case, where the law in force in the third country or applicable to the international organisation does not guarantee an adequate level of protection of personal data, the transfer may only be carried out subject to the adoption of additional security measures suitable to mitigate the risks to the rights and freedoms of the data subjects (eg, encryption of the data prior to the transfer in order to exclusively share encrypted data).

With reference to *non-personal data*, see 5.2 Government Notifications and Approvals and 5.3 Data Localisation Requirements.

5.2 Government Notifications and Approvals

With reference to *personal data*, notification to the supervisory authority is only required in the case of transfers pursuant to Article 49 (1)(2) of the GDPR. This is the case when no other means can be used to legitimise the transfer, and requires that the transfer:

- is not repetitive;
- concerns a limited number of data subjects;
- is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject;
- is carried out subject to appropriate data protection safeguards; and
- is notified to the supervisory authority by the data controller.

With reference to *non-personal data*, Article 32 of the Data Act works as a safeguard against third-country authorities trying to obtain non-personal data stored in the EU from cloud/data-processing providers. A foreign court order or administrative decision is enforceable in the EU only if it is based on an international agreement with the EU or a member state (for example, a mutual legal assistance treaty). If no such agreement exists and compliance would conflict with EU or national law, the provider may grant access only where the third-country legal system offers solid rule-of-law guarantees:

- the order must be reasoned, specific and proportionate;

- the provider must be able to object and obtain judicial review; and
- the reviewing court must be empowered to take account of the provider's EU-protected interests.

To assess this, the provider can ask for an opinion from the national authority competent for international legal co-operation, especially where the request concerns trade secrets, commercially sensitive data, IP-protected material, or risks of re-identification; that authority may consult the Commission. A similar check applies if national security or defence interests may be involved. If the authority does not respond within one month, or concludes that the safeguards are not met, the provider is entitled to refuse the foreign request.

5.3 Data Localisation Requirements

With reference to *personal data*, European legislation on the protection of personal data does not provide for any obligation to store data within a specific member state or the EEA, aiming, on the contrary, to regulate and facilitate the free movement of such data. In the case of transfers of data to third countries, however, the provisions of Chapter V of the GDPR apply in order to guarantee an adequate level of protection of personal data (see 5.1 Restrictions on International Data Transfers).

With reference to *non-personal data*, Article 32 of the Data Act states that the providers of data processing services shall take all adequate technical, organisational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the EU where such transfer or access would create a conflict with Union law or with the national law of the relevant member state.

5.4 Blocking Statutes

There are no “blocking” statutes in European legislation in addition to those described in the previous sections concerning the transfer of data outside the EEA.

5.5 Recent Developments

The most recent update was in 2024, when the European Commission concluded the review process of 11 adequacy decisions regarding the transfer of personal data, confirming their validity. In this regard, the decisions remain effective, and it is permissible to continue the free transfer of personal data to Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

Trends and Developments

Contributed by:

Paolo Balboni, Luca Bolognini, Davide Baldini and Nicolò Maria Salvi
ICT Legal Consulting

ICT Legal Consulting (ICTLC) is an international law firm that provides strategic legal and regulatory support across privacy, data protection, intellectual property, and technology, media and telecommunications (TMT) law, with a strong focus on the normative and operational aspects of cybersecurity. The firm assists organisations in designing and implementing governance, compliance and security frameworks that meet the highest international standards. With over 80 professionals and a network active in more than 65 juris-

dictions, ICTLC combines global co-ordination with local insight. Through its sister company ICT Cyber Consulting, the firm offers integrated cybersecurity services, including legal-technical risk assessments, resilience planning, and alignment with frameworks such as NIS2, DORA and the Cyber Resilience Act. ICTLC's multidisciplinary expertise enables clients to navigate complex digital regulations and strengthen trust, compliance and resilience across their global operations.

Authors



Paolo Balboni is a leading European ICT, privacy and cybersecurity lawyer, serving as the Data Protection Officer for multinational companies. Admitted to the Milan and Amsterdam Bars, he is founding partner of ICT Legal

Consulting and ICT Cyber Consulting. He advises on legal matters involving data protection, cybersecurity, AI, IoT, IT contracts and digital regulation. Paolo is a professor at Maastricht University, and holds positions with the EPO and European Commission expert groups. He is a published author and frequent keynote speaker. His expertise spans multiple sectors, and he has contributed to key EU regulatory frameworks, including the GDPR and cloud data protection codes.



Luca Bolognini is a prominent privacy and data protection attorney, admitted to the Italian Supreme Court, and is founding partner of ICT Legal Consulting. He serves as President of the Italian Institute for

Privacy and Data Valorisation, co-founded several cybersecurity ventures, and directs Giuffrè Francis Lefebvre's "IUS Privacy Portal". Recognised internationally by Chambers Europe, Luca frequently contributes to European research initiatives, teaches at numerous prestigious universities, and actively publishes influential works addressing privacy, data protection, cybersecurity, artificial intelligence and digital innovation. His extensive scholarship emphasises balancing technological advancement with robust legal and ethical frameworks.



Davide Baldini is a lawyer and managing partner of ICT Legal Consulting. He advises multinational companies and innovative start-ups on data protection and IT contracts.

He is a qualified Data Protection Officer (ECPC-B) from Maastricht University, and a certified auditor for the Cloud Security Alliance Code of Conduct and the Europrivacy Certification Scheme. He is the author of several essays and articles for legal blogs and top-tier law journals. He is a PhD candidate in International and European Law at the University of Florence, where he is working on artificial intelligence and algorithmic discrimination.



Nicolò Maria Salvi has been advising on personal data protection and ICT law since 2017, with a focus on data protection compliance and legal issues related to the use of new technologies. He is a partner at ICT

Legal Consulting, a certified Data Protection Officer and a certified auditor under the Europrivacy certification scheme. He holds a master's degree in Data Protection and Data Protection Design, and is enrolled in the Register of the Italian Institute for Privacy and Data Valorisation. He also serves as assistant professor in Constitutional and Media Law at LUISS Guido Carli University.

ICT Legal Consulting

ICT Legal Consulting
Via Borgonuovo 12
20121 Milan
Italy

Tel: +39 0284 2471 94
Fax: +39 0270 05121 01
Email: info.legal@ictlc.com
Web: www.ictlegalconsulting.com



Data Protection Enforcement Trends in Italy

Overview

Article 51 of the General Data Protection Regulation (GDPR) provides that “each member state shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union”. Under Article 58 GDPR, the supervisory authority is granted a wide range of powers, including investigative, corrective, authorising and advisory powers, among which is – notably – the possibility to levy pecuniary fines and to impose a temporary or definitive ban on the processing of personal data.

In Italy, the competent supervisory authority is the *Garante per la Protezione dei Dati Personali* (so-called “Garante”, or GPDP), whose decisions can be appealed by applying to the ordinary tribunal on second degree, and to the Supreme Court of Cassation on third degree.

The GPDP is widely considered one of most active and influential supervisory authorities, having issued – as of 31 December 2025 – more than 575 publicly available enforcement actions, amounting to over EUR315,696,105 in sanctions. This leaves Italy behind only Spain in terms of the number of sanctions issued, given that the Spanish supervisory authority has issued at least 1,027 sanctions, though levying only a total amount of approximately EUR137,721,810 in sanctions. The GPDP has issued fines and leveraged its corrective powers – including the imposition of a ban on processing – towards most GDPR areas and industry sectors. There are, however, aspects of the GDPR on which the authority seems to focus its attention more often than others.

Trends in Enforcement

Traditionally, the GPDP has been especially concerned with combating unlawful telemarketing practices, in particular as regards transparency and consent requirements as well as the engagement of third parties (such as call centres) as data processors without the necessary data protection safeguards, including performance of audits by the data controller. In this

field, the GPDP has issued some of its highest sanctions ever published, such as those against Eni Gas e Luce (issued on 11 December 2019, for a total amount of EUR11.5 million), Tim (issued on 15 January 2020, for a total amount of EUR27.8 million) and Sky Italia (issued on 16 September 2021, for a total amount of EUR3.2 million). More recently, in July 2024, the GPDP ordered Hera (an energy provider) to pay a fine of EUR 5 million for violations in the processing of personal data of over 2,300 customers due to the insufficient implementation of safeguards by Hera’s data processors, which in some cases had led to the activation of energy supply contracts without knowledge or consent from the users.

During the last few years, the GPDP has also focused its attention on the protection of the data privacy rights of children, as apparent from the enforcement actions undertaken against the popular social network TikTok concerning data verification requirements. On 22 January 2021, following the highly publicised death of a ten-year old girl from Sicily participating in a “blackout” challenge, the GPDP imposed an immediate limitation on the data processing concerning users “whose age could not be established with full certainty so as to ensure compliance with the age-related requirements”. On 3 February 2021, the GPDP noted that, following the enforcement action, TikTok committed to fulfilling GDPR age-verification requirements by taking a number of actions, including:

- removing accounts belonging to users under 13 years of age;
- employment of an AI-based system to verify age;
- launching an information campaign to raise awareness;
- including an in-app button for reporting those under 13 years of age;
- improving the language of the privacy notice for users under 18 years of age; and
- doubling the number of Italian platform content moderators.

Another field where the GPDP has recently stepped up its enforcement actions is that of video-surveillance. In October 2023, the GPDP reprimanded an individual person for installing a home surveillance system with cameras capturing not only their own apartment but

also a public area (including a public park). According to the GPDP, the placement of the cameras violated the principle of lawfulness, as the data controller failed to show a legitimate interest capable of justifying the recording of public areas and conversations through the audio system, as well as the principle of data minimisation. The decision is also interesting because it clarifies that, while domestic surveillance systems are generally exempt from having to comply with the GDPR, such exemption does not apply when involving public or third parties' properties. The GPDP issued a mere reprimand against the data controller, considering that the individual promptly rectified the situation by replacing the camera and redirecting it solely towards the entrance of their home.

In June 2023, the GPDP issued a sanction of EUR20,000 against an Italian employer for, inter alia, having installed a video-surveillance system in its premises without having obtained the prior approval of the workers' council or of the public labour authority, as required by Article 4 of Law No 300/1970 (the so-called "Workers' Statute"). Moreover, no privacy notice had been drafted and made available to the workers. More recently, in July 2024, the GPDP ordered the Turin municipality to share further information relating to the use of AI-powered "smart CCT-Vs", which would allegedly help local police forces to understand whether their intervention is needed in emergency situations, in order for the GPDP to be able to investigate the system's compliance with the GDPR.

Lastly, a field where the GPDP has focused much of its attention since early 2023 is that of artificial intelligence (AI), as shall be seen specifically in the following section.

The GPDP at the Forefront of AI Enforcement

During the last couple of years, the GPDP has taken noteworthy initiatives in the context of AI, including by means of enforcement actions against major providers of generative AI systems and models. As a result, the GPDP has accredited itself as one of the most active EU supervisory authorities on the regulation of AI vis-à-vis the GDPR and the Italian Data Protection Law. The following provide a brief overview of the

most important initiatives undertaken by the GPDP in the AI field.

Enforcement action against OpenAI

In late March 2023, only a few months after its launch, the GPDP identified several violations of the GDPR and the Italian Data Protection Law regarding the famous and widespread generative AI system ChatGPT. According to the GPDP, OpenAI failed to demonstrate the presence of a valid legal basis for collecting and processing personal data for the purposes of training ChatGPT, and the information provided to users and individuals whose data was used for training the generative AI system was incomplete. Moreover, individuals whose data was used for training the AI system had no easy way to exercise their data protection rights, including the rights of access, rectification and objection. Interestingly, the GPDP also noted that ChatGPT's responses to users' prompts often deviated from reality (so-called "hallucinations"), thereby violating the accuracy principle established by the GDPR when such responses concerned another individual. The ChatGPT case further underscores, once again, the GPDP's scrutiny of data processing concerning children: in this respect, the authority questioned whether the platform's outputs might result in inappropriate responses for children, even if the service is purportedly aimed at users above the age of 13, as stated in OpenAI's terms of service. As a result, the GPDP required OpenAI to implement a suitable age verification system.

On 28 April 2023, the GPDP lifted the ban, as it considered the measures adopted by OpenAI to adequately address the data protection issues raised by the authority and which underpinned the ban. Such measures included updating ChatGPT's privacy policy, implementing adequate age-verification systems, and implementing measures to enable individuals to exercise their data protection rights. However, the GPDP reserved its powers to fully investigate the underlying shortcomings that led to it issuing the ban in the first place and, if necessary, issuing any relevant sanction in a separate decision after having fully investigated the facts.

The final decision was issued on 2 November 2024. In its ruling, the GPDP imposed a EUR15 million fine

on OpenAI and mandated the company to launch a six-month public awareness campaign. The campaign should be aimed at educating the public about the collection of personal data for training its generative AI model ChatGPT, and informing individuals about their data protection rights (such as the right to opt out).

The amount of the fine was due to the following data protection infringements by OpenAI.

- Processing personal data without having previously identified a suitable legal basis.
- Lack of age-verification mechanisms. When the service launched, there were no effective measures to verify users' ages.
- Failure to implement the campaign to raise awareness in the way prescribed by the GPDP within the 2023 provisional decision.
- Provision of insufficient information to users within ChatGPT's privacy notice, especially as regards the failure to inform data subjects about how their personal data was processed, including its use for training the AI model.
- Violation of the accuracy principle, as ChatGPT's responses often result in incorrect information about individuals.

The fine considered OpenAI's co-operative approach, acknowledging the implementation of several measures requested by the GPDP. OpenAI was given 30 days to pay the fine and 60 days to submit a detailed plan for the required awareness campaign to the GPDP.

The GPDP–OpenAI saga has garnered widespread attention, not only within the Italian data protection community but also in the general public of both Italy and Europe, given that it is one of the first enforcement initiatives to have targeted a generative AI system. The GPDP activity goes to show the GDPR potential of regulating specific aspects relating to generative AI, as well as the GPDP's willingness to lead the way in this respect.

Finally, given that during the investigation OpenAI established its EU headquarters in Ireland, the Irish Data Protection Commissioner (DPC) was brought into focus as the lead supervisory authority for OpenAI.

In line with the GDPR's one-stop-shop mechanism, the GPDP has forwarded the case documents to the DPC, which will now be responsible for investigating any further data protection infringements involving OpenAI.

Enforcement action against DeepSeek

DeepSeek entered the global AI market in January 2025, attracting widespread attention as the first large-scale Chinese generative AI model capable of competing with leading US providers. Its launch was widely perceived as a turning point in the AI market, both for its technological ambitions and for the broader geopolitical implications of a non-US model achieving comparable performance and, in some cases, adoption at international level.

The GPDP once again positioned itself at the forefront of regulatory enforcement in the AI sector. The authority promptly initiated supervisory action against the companies operating the service, confirming its determination to play a leading role in asserting the application of EU data protection rules to global AI providers, irrespective of their place of establishment.

In January 2025, a few days after DeepSeek's launch, the GPDP adopted urgent measures against Hangzhou DeepSeek Artificial Intelligence Co, Ltd and Beijing DeepSeek Artificial Intelligence Co, Ltd, the Chinese companies operating the generative AI service known as DeepSeek. The service is offered through a website, applications and related software, and allows users to access AI-driven functionalities after registration.

The case originated from a formal request for information sent by the GPDP to the companies on 28 January 2025. In their reply, they stated that DeepSeek had not entered, nor intended to enter, the Italian market and that the application had been removed from Italian app stores. The companies also argued that the GDPR did not apply to their processing activities. Following a rapid investigation, the GPDP established that, although DeepSeek's mobile app was no longer available on the Apple and Google App Stores in Italy, the underlying service remained accessible to Italian users through its website. In addition, users who had previously registered were still able to log in and use

the service. On this basis, the authority concluded that DeepSeek was unquestionably offering its services to individuals located in the EU, including Italy. As a consequence, the GPDP found that the GDPR applied extraterritorially on the basis of its Article 3 (2), as the service targeted individuals residing in the Union. The authority also noted that DeepSeek had failed to co-operate adequately with the investigation, having omitted to clarify key aspects of its data processing activities, therefore breaching its co-operation duties laid down in Article 31 GDPR.

Several substantive shortcomings were also identified. DeepSeek's privacy policy was not available in Italian, but only in English, and did not meet the transparency and information requirements set out in Articles 12, 13 and 14 of the Regulation, as it missed a few mandatory requirements. In particular, it failed to clearly specify the legal bases relied upon for each processing activity, contrary to Article 6 GDPR, and did not provide sufficient information to enable data subjects to exercise their subjective data protection rights (eg, access, rectification, objection, portability, deletion, etc).

Further concerns arose in relation to international data transfers and security. According to the privacy policy, personal data collected through the DeepSeek service were stored in the People's Republic of China, without adequate safeguards being demonstrated, raising issues under the data transfers regime foreseen by the GDPR, as strictly interpreted by the Court of Justice (most famously in the *Schrems I* and *Schrems II* judgments).

Finally, despite being subject to the GDPR while being established in a third country, the companies had failed to appoint a representative in the EU, in violation of Article 27.

Given the seriousness of the findings and the ongoing nature of the investigation, the GPDP ordered, on an urgent basis, a definitive limitation on the processing of personal data of individuals located in Italy. The measure took immediate effect and was adopted without prejudice to any further enforcement action that may follow upon completion of the investigation.

Once again, the decision illustrates the GPDP's readiness to intervene swiftly in the AI domain and its ambition to remain a key EU data protection enforcer vis-à-vis global AI providers.

Enforcement in the Field of Data Brokering Services

Inquiry regarding Lusha

Aside from the AI sector, the GPDP has also recently concentrated its efforts on enterprises providing data brokering services to the Italian market.

One salient example is the enforcement action against Lusha Systems Inc, a US-based company that operates an online platform offering so-called "enriched" contact data of potential leads. Through subscriptions purchased by its clients – typically sales, marketing and recruitment professionals – the platform allows users to identify or verify business contact details such as email addresses, landline numbers and mobile phone numbers of potential leads, including professionals and other individuals working for companies that may be interested in their services, with a view towards contacting them by leveraging the contact data provided by Lusha.

Lusha's services are built around personal data-gathering and aggregation from multiple sources, including work-related social networks, websites of companies, and many other third-party sources. The service therefore does not only include registered users of the platform, as the database may also include personal data relating to individuals who have never interacted with Lusha directly.

Importantly from a jurisdictional perspective, the GPDP found that Lusha's services are accessible from the EU and are actively offered to users located in EU member states, including Italy. Lusha's database reportedly contains personal data relating to EU residents, including Italian residents and, in some cases, individuals holding prominent institutional or senior professional roles. This circumstance was decisive in allowing the GPDP to assert its jurisdiction vis-à-vis Lusha.

On 8 April 2025, the GPDP formally announced the opening of an investigation into Lusha. The decision

followed multiple complaints from individuals who reported receiving unsolicited promotional or commercial telephone calls allegedly made using contact details obtained through Lusha's services. According to the GPDP, preliminary information suggested that Lusha was selling contact details, including telephone numbers, some of which appeared to be of uncertain or problematic origin in light of the GDPR. The authority also highlighted that Lusha's database included data relating to Italian residents, and that the platform was being used by companies to carry out marketing activities targeting individuals in Italy.

In light of the above, the GPDP issued a formal request for information to Lusha, requiring the company to respond within 20 days from receipt thereof. The request was broad in scope and aimed at clarifying the fundamental aspects of Lusha's data processing activities in so far as they affect individuals in Italy.

In particular, the authority asked Lusha to provide:

- details on the quantity of personal data relating to individuals residing in Italy that is collected or processed;
- a clear description of the means used to collect such data;
- comprehensive information on each source contributing to the database;
- clarification as to whether personal data of individuals who are not platform users is processed; and
- specific information, with regard to email addresses and telephone numbers, on the relevant sources, consent mechanisms and purposes of data-sharing with platform users.

Moreover, the GPDP recalled that similar business models had already been under scrutiny in the past. In earlier cases, the authority had sanctioned real estate agencies for carrying out promotional activities using telephone numbers purchased from third-party providers that were offering services comparable to those provided by Lusha.

On 5 December 2025, the GPDP issued a further communication, clarifying that the proceedings which had been promptly opened in April 2025 were still fully ongoing. The GPDP confirmed that its investigation

had been triggered in light of the receipt of formal complaints from data subjects who lamented having received unwanted promotional or commercial calls based on data included in Lusha's database.

From the authority's preliminary findings, it emerged that Lusha collects and processes personal data of EU residents, building its services around the collection and further sharing of this data with potential clients, while maintaining that compliance with data protection rules rests primarily with the latter, as data controllers.

The GPDP also highlighted that Lusha includes in its services the contact details of public figures, including individuals holding public and institutional positions. This element raises additional concerns in light of the principles of lawfulness, purpose limitation and data minimisation, as well as in light of the data subjects' increased expectations of privacy and transparency applicable when processing personal data at scale.

It is worth noting that, although Lusha operates across all EU member states, the GPDP is, at present, the only supervisory authority to have formally launched an in-depth investigation into the platform. This confirms the proactive stance traditionally adopted by the Italian authority in sectors perceived as high-risk, including telemarketing, the commercial trading of personal data and – as seen above – AI.

At the same time, the GPDP has made it clear that its enforcement focus is not limited to Lusha alone. The authority is monitoring other major platforms active in the personal contact data market, and is also assessing the position of companies that have relied on such databases to carry out marketing activities without an adequate legal basis.

The outcome of the Lusha investigation may therefore have significant implications, not only for the company and its clients themselves but also for the wider ecosystem of data brokers, and for businesses that source contact data from third-party providers and/or publicly available sources (such as social networks and public databases).

This case serves as a reminder that the commercial value of leveraging third-party-managed large-scale contact databases and the possibility of relying on data-brokering services always require a careful assessment of compliance with EU data protection rules, and that offering or receiving similar services may entail some level of compliance risk.

Contributed by:

Samantha Moore, Marc Ramsay and Chantelle Biersay
Ramsay & Partners



Contents

1. Legal and Regulatory Framework p.223

- 1.1 Overview of Data and Privacy-Related Laws p.223
- 1.2 Rights and Obligations p.223
- 1.3 Special Categories of Personal Data p.225
- 1.4 Processing of Personal Data for Research and Development Purposes p.226
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.227
- 1.6 Data Breach Requirement p.227
- 1.7 Regulators p.227
- 1.8 Enforcement Proceedings and Fines p.228
- 1.9 Enforcement Trends p.229

2. Privacy Litigation p.229

- 2.1 Privacy Litigation Overview p.229
- 2.2 Recent Case Law p.229
- 2.3 Collective Redress Mechanisms p.230

3. Requirements for the Protection and Processing of Non-Personal Data p.230

- 3.1 Objectives and Scope of Data Regulation p.230
- 3.2 Interaction of Data Regulation and Data Protection p.230
- 3.3 Rights and Obligations Under Applicable Data Regulation p.230
- 3.4 Regulators and Enforcement p.230

4. Sectoral Topics p.230

- 4.1 Use of Cookies p.230
- 4.2 Personalised Advertising and Other Online Marketing Practices p.230
- 4.3 Employment Privacy Law p.230
- 4.4 Data Protection in M&A p.231

5. International Considerations p.232

- 5.1 Restrictions on International Data Transfers p.232
- 5.2 Government Notifications and Approvals p.232
- 5.3 Data Localisation Requirements p.232
- 5.4 Blocking Statutes p.232
- 5.5 Recent Developments p.232

Ramsay & Partners is a full-service law firm comprising six lawyers with a dedicated data protection and cybersecurity practice, led by a partner and supported by corporate, regulatory, employment and technology specialists. The firm is headquartered in Kingston, Jamaica, and is the exclusive member for Jamaica of the Chambers Band 1-ranked TerraLex global legal network, enabling structured multi-jurisdictional co-ordination across the Caribbean and key international markets. The practice advises on compliance with the Jamaica Data Protection Act, privacy governance, cybersecurity incident response, cross-border data transfers, and data protection is-

sues arising in corporate transactions, employment structures, fintech and regulated industries. Its work frequently intersects with governance, regulatory compliance and risk management. Recent matters include advising multinational technology companies on Jamaican data protection compliance and breach response, co-ordinating regional advice for cross-border operations, supporting financial services providers with data governance frameworks, and advising employers and healthcare-related entities on lawful processing, retention and regulatory engagement.

Authors



Samantha Moore is a partner at Ramsay & Partners and leads the firm's data protection and cybersecurity practice. She advises on compliance with the Jamaica Data Protection Act and related regulatory

frameworks, including cross-border data protection issues and cybersecurity incident response. Her experience includes advising some of the world's largest technology companies as they navigate data protection obligations in Jamaica, including regulatory engagement and data breach response. She was called to the Jamaican Bar in December 2012 and joined the partnership in December 2020, having previously practised at a major Caribbean firm. Samantha is a member of the Jamaican Bar Association and serves on its Commercial Law and Telecommunications, Broadcasting & Technology subcommittees.



Marc Ramsay is the managing partner of Ramsay & Partners and supports the firm's data protection and cybersecurity practice through his work in governance, regulatory and compliance advisory. He advises

boards, regulators and senior management on organisational accountability, risk oversight and compliance structures, including where data protection obligations intersect with corporate

governance, financial services regulation and cross-border operations. His experience includes advising on regulatory engagement, internal control frameworks and compliance risk allocation for technology-enabled and regulated businesses. Marc is admitted to practice in Jamaica, Belize and Barbados. He is a member of the Jamaican Bar Association and is a Professionally Accredited Company Secretary, with longstanding experience advising boards on governance and regulatory compliance matters.



Chantelle Biersay is an associate at Ramsay & Partners and supports the firm's data protection and cybersecurity practice alongside her corporate and commercial work. She assists on data protection compliance

matters, including regulatory analysis, policy implementation, and advisory work where data protection issues arise in commercial transactions and operational structures. Her broader experience includes corporate transactions, real estate, conveyancing and capital markets work, including high-value secured facilities for financial institutions. Chantelle was admitted to practice in Jamaica in 2020 and New York in 2025. She holds a Master of Laws in Corporate and Commercial Law and is a member of the Jamaican Bar Association.

Ramsay & Partners

8 Lady Musgrave Road
Kingston 5
St Andrew
Jamaica

Tel: +1 876 906 2616
Email: inbox@ramsayandpartners.com
Web: jamaicadataprotection.com



RAMSAY & PARTNERS

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The following laws and/or regulations govern data protection and privacy in Jamaica:

- the Data Protection Act, 2020 (DPA);
- the Data Protection Regulations, 2024 (the “Regulations”); and
- the Data Protection (Data Controller Registration) Regulations, 2024 (the “Registration Regulations”).

In Jamaica, these laws are the only set which govern data protection and privacy. Our laws do not distinguish between federal and state, nor do we have laws that distinguish between the national and subnational, the supranational and domestic, or the general and sectoral.

The DPA is extraterritorial in scope in that it applies to individuals and/or entities that are not resident or established in Jamaica but:

- use equipment in Jamaica for the processing of personal data other than for the purpose of transit through Jamaica; or
- process personal data of data subjects in Jamaica, and the processing activities relate to:
 - (a) the offering of products or services to data subjects in Jamaica, irrespective of whether a payment is required; or
 - (b) the monitoring of the behaviour of data subjects to the extent that their behaviour takes place within Jamaica.

Interplay Between the DPA and Other Laws *Cybercrimes Act*

The Cybercrimes Act, 2015 supports the DPA’s security goals by criminalising unauthorised access and interference with systems and data.

A data breach under the DPA may also constitute an offence under the Cybercrimes Act, for example, unauthorised access, which has the potential to create dual civil and criminal liability.

The Cybercrimes Act applies to all data and is not limited to personal data. This means that it covers criminal misuse of non-personal data such as corporate data held on IT systems.

1.2 Rights and Obligations *General Principles*

All data controllers are required to comply with the eight data protection standards set out under the DPA. These data protection standards are as follows:

- *Fairness and lawfulness*: Personal data must be processed fairly and lawfully and must not be obtained by deception or any misleading information.
- *Purpose limitation*: Personal data must only be obtained for a specific and lawful purpose and must not be processed in any manner incompatible with those purposes.
- *Data minimisation*: Personal data must be adequate, relevant, and limited to the purpose for which it is being processed.
- *Accuracy*: Personal data must be accurate and, where necessary, kept up to date.

- *Storage limitation:* Personal data must not be kept for longer than is necessary and must be disposed of in accordance with any regulations (once passed) under the DPA.
- *Rights of data subject:* Personal data must be processed in accordance with the rights of the data subject;
- *Implementation of technical and organisational measures:* Personal data must be protected using appropriate technical and organisational measures so as to prevent unauthorised or unlawful processing of the data as well as any accidental loss or destruction of, or damage to, the data.
- *Cross-border transfers:* Personal data must not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data.

Conditions for Processing Personal Data

The DPA stipulates that personal data must not be processed unless at least one of the following conditions has been met:

- the data subject has consented to the processing and has not withdrawn that consent;
- the processing is necessary (i) for the performance of a contract to which the data subject is a party; or (ii) for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
- the processing is necessary in order to protect the vital interests of the data subject;
- the processing is necessary (i) for the administration of justice; (ii) for the exercise of any functions conferred by or under any enactment; or (iii) for the exercise of any other functions of a public nature exercised in the public interest;
- the processing is necessary for the purposes of legitimate interests pursued by the data controller or by any third party to whom the personal data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice

to the rights and freedoms or legitimate interests of the data subject; or

- the data subject has published the personal data concerned.

Data Subject Rights

Right to be informed/right to access

A data subject has the right to be informed of whether his/her personal data is being processed by or on behalf of the data controller, and if so, he/she has the right to be provided with:

- a description of the personal data;
- the purposes for which the data is being processed; and
- the recipients to whom the disclosure is made.

Right to rectification

A data subject has the right to request that the data controller rectify any inaccuracy in his/her personal data which is in the data controller's possession or control. For the purposes of the DPA, the term "rectify" means to amend, block, erase or destroy and the term "inaccuracy" includes any error or omission.

The right to prevent processing

A data subject has the right to prevent the processing of his/her personal data in specified circumstances such as:

- where the processing is likely to cause substantial damage or substantial distress to the data subject or to another person and where the damage or distress caused or likely to be caused (as the case may be) is unwarranted;
- where the processing of the data is incomplete or irrelevant;
- where the processing of the data is prohibited by law; or
- where the data has been retained by the data controller for a period longer than required by law.

The right to prevent processing for direct marketing purposes

A data subject has the right to prevent the processing of his/her personal data for the purposes of direct marketing unless the data subject gives his/her consent or is a customer of the data controller.

Right not to be subject to automated decision-making

A data subject has the right to request that a data controller does not make any decision which would significantly affect him/her solely on the basis of the results of automated processing. These decisions include matters relating to the evaluation of the data subject's work performance, creditworthiness, reliability or conduct.

Compliance Checklist

Below is a detailed checklist of the "to dos" for organisations under the DPA.

Registration and record-keeping

All data controllers are required to register with the Information Commissioner before processing personal data. Data controllers must pay the prescribed registration fee and annual maintenance fee to keep the registration active.

Data controllers are also required to provide and maintain detailed processing records, including:

- data controller's name/contact details;
- description of personal data processed;
- categories of data subjects;
- purpose(s) of processing; and
- recipients of personal data (including transfers abroad).

Data protection impact assessment

Unless otherwise indicated by the Information Commissioner, data controllers are required to annually submit to the Information Commissioner a data protection impact assessment (DPIA) in respect of all personal data in the custody or control of the data controller.

Data Protection Officer (DPO)

Data controllers that fall within any of the following categories are required to appoint a DPO:

- data controllers that are public authorities;
- data controllers that process or intend to process sensitive personal data or data relating to criminal convictions;

- data controllers that process personal data on a large scale; and
- data controllers that are designated by the Information Commissioner as requiring a DPO.

Compliance with data protection standards

All data controllers must comply with the eight data protection standards as outlined in the DPA. These standards are discussed above.

Breach notification

All data controllers are required to report any security breach in respect of the data controller's operations which affects or may affect personal data to the Information Commissioner within 72 hours after becoming aware of the breach.

Data controllers are also required to report any security breach to each data subject whose personal data has been affected by such breach within 72 hours after becoming aware of the breach.

Incident and breach management

Data controllers are required to maintain records of breaches and any remedial actions taken.

1.3 Special Categories of Personal Data

Conditions for Processing Sensitive Personal Data

The DPA stipulates that sensitive data must not be processed unless at least one of the following conditions has been met:

- the data subject has consented in writing to the processing of the personal data;
- the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred, or imposed, by law on that data controller in connection with employment or social security benefits;
- the processing is necessary:
 - (a) in order to protect the vital interests of the data subject or another individual, in any case where:
 - (i) consent cannot be given by or on behalf of the data subject; or
 - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, the data controller having

- exhausted all reasonable efforts to obtain that consent; or
 - (b) in order to protect the vital interests of another individual, in any case where consent by or on behalf of the data subject has been unreasonably withheld;
- the processing:
 - (a) is carried out in the course of legitimate actions by any body or association which:
 - (i) is not established or conducted for profit; and
 - (ii) exists for political, philosophical, religious or trade-union purposes;
 - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
 - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
 - (d) does not involve disclosure of personal data to a third party without the consent of the data subject;
- the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;
- the processing:
 - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (b) is necessary for the purpose of obtaining legal advice; or
 - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- the processing is necessary for:
 - (a) the administration of justice; or
 - (b) the exercise of any functions conferred on any person by or under any enactment;
- the processing is:
 - (a) either:
 - (i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such organisation; or
 - (ii) any other processing by a person referred to in (i) above or another person of sensitive personal data so disclosed; and
 - (b) necessary for the purpose of preventing fraud;
- the processing is necessary for medical purposes and is undertaken by:
 - (a) a health professional; or
 - (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional; or
- (a) the processing: (i) is of sensitive personal data consisting of information as to racial or ethnic origin; (ii) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between individuals of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and (iii) is carried out with appropriate safeguards for the rights and freedoms of data subjects; or (b) the sensitive personal data is processed in circumstances specified in an order made by the relevant Minister.

Children's Data

The DPA states that where the personal data being processed belongs to a minor, the rights granted to a data subject under the DPA may be exercised by a parent or legal guardian of the minor, or by the minor in any case where the law recognises the capacity of the minor to act on his/her own behalf.

The DPA also stipulates that where consent is required for processing, in the case of a minor, the consent must be given by a parent or legal guardian of the minor, unless the law recognises the capacity of the minor to give consent on his/her own behalf.

1.4 Processing of Personal Data for Research and Development Purposes

The DPA is silent with respect to the anonymisation of patient data for the purposes of product development or scientific research.

Note, however, that where the personal data is anonymised so that no individual can be personally identifiable from the information, the DPA would not be applicable. In those circumstances, the data can be used for product development or scientific research purposes.

Additionally, the DPA stipulates that personal data can be processed for research purposes so long as the following conditions are met:

- the personal data must not be processed to support measures or decisions with respect to particular individuals; and
- the personal data must not be processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

In Jamaica, we are not familiar with the European Health Data Space Regulation, nor do we have similar laws.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

In Jamaica, we have not yet implemented specific requirements or guidance regarding the use of personal data in AI systems or models. Likewise, Jamaica does not yet have a comprehensive AI regulatory regime.

1.6 Data Breach Requirement

A data controller is required to report any security breach in respect of the data controller's operations that affects or may affect personal data to the Information Commissioner within 72 hours of becoming aware of the breach. The notice must include:

- the facts surrounding the security breach;
- a description of the nature of the security breach, including the categories, the number of data subjects concerned, and the type and amount of personal data concerned;
- the measures taken or proposed to be taken to mitigate or address the possible adverse effects of the breach;
- the consequences of the breach; and
- the name, address and other relevant contact information of the data controller's DPO.

The notice must be submitted via the Information Commissioner's online portal.

A data controller is also required to report any security breach to each data subject whose personal data has been affected by such breach within 72 hours

of becoming aware of the breach. The notice must include:

- the nature of the security breach;
- the measures taken or proposed to be taken to mitigate or address the possible adverse effects of the breach; and
- the name, address and other relevant contact information of the data controller's DPO.

Please note that as the DPA was only recently implemented, the investigative arm of the Information Commissioner has not yet been fully established. Additionally, the provisions under the DPA which give the Information Commissioner certain enforcement powers are not yet in effect.

In Jamaica, mass data privacy litigation is not common.

1.7 Regulators

The Information Commissioner is the regulatory body which is designated to enforce the DPA and handle complaints, investigations, penalties and compliance.

The main powers, duties and responsibilities of the Information Commissioner include:

- monitoring compliance with the DPA and any regulations made thereunder;
- providing advice to the relevant Minister on any matter relating to the operation of the DPA or otherwise for the protection of personal data;
- promoting the observance of the requirements under the DPA and the following of good practice by data controllers;
- disseminating information to the public about the operation of the DPA and about good practice, and advising persons about any of those matters;
- preparing and disseminating guidelines under the DPA; and
- intervening as a party in any proceedings before a court, in respect of any matter concerning the processing of personal data or the enforcement of any provision of the DPA, other than proceedings for the prosecution of an offence.

Where the Information Commissioner is satisfied that a data controller has contravened, or is contravening, any of the provisions under the DPA, the Information Commissioner may commence proceedings against the data controller. Proceedings may also be triggered where a data subject has filed a complaint with the Information Commissioner against a data controller.

Guidelines issued by the Information Commissioner pursuant to the DPA would be binding in practice.

1.8 Enforcement Proceedings and Fines

How an Enforcement Action or Investigation is Initiated

Any person who believes his/her rights under the DPA have been violated can lodge a complaint with the Information Commissioner, which would then trigger an investigation by the Information Commissioner.

The Information Commissioner may commence an investigation on its own initiative in circumstances where there is reason to suspect non-compliance by a data controller (for example, a serious breach, public interest concerns, or patterns of misconduct).

Investigations may also be triggered through referrals or media reports.

Enforcement Notices

If the Information Commissioner has reasonable grounds for believing that a data controller is non-compliant with the DPA, the Information Commissioner has the power to issue an enforcement notice to such data controller. This enforcement notice may require the data controller to cease processing, correct practices, or take specific steps to comply with the DPA. The enforcement notice typically sets a compliance deadline by which the data controller must act.

Information and Assessment Notices

The Information Commissioner has the power to issue information notices which would require data controllers to produce certain documents or evidence related to compliance. This would also give the Information Commissioner the power to inspect the data controllers' premises, books, etc.

A request may also be made to the Information Commissioner by or on behalf of any individual who is, or believes himself/herself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been, or is being, carried out in compliance with the DPA.

Notice of Investigation

When an investigation begins, the Information Commissioner will typically provide formal notice to the data controller that an inquiry has been opened.

The notice should explain the scope of the investigation, the alleged non-compliance and any documentation required.

Response Timelines

The DPA generally requires data controllers to respond to the Information Commissioner requests within specified timeframes.

For example, data controllers are required to respond to data subject access requests within 30 days from the date of the request.

Available Sanctions and Remedies

Where a body corporate commits an offence under the DPA, the body corporate may be liable to a fine not exceeding 4% of its annual gross worldwide turnover of that body corporate for the preceding year of assessment in accordance with the Income Tax Act, 1955 (as amended).

Individuals who commit an offence under the DPA may also be subject to severe fines up to a maximum of JMD5 million (approx. USD31,100) and/or imprisonment up to a maximum of ten years.

In calculating the amount of monetary penalties, the courts will take into account:

- the estimated economic cost to consumers, users of the services concerned and any other persons, of the contravention giving rise to the offence;
- the estimated economic benefit derived by the body corporate from the commission of the offence;

- the period for which the contravention continued;
- the number and severity of any other offences under the DPA committed by the body corporate; and
- any other factors which the court considers relevant.

An individual who suffers damage by reason of any contravention by a data controller of any of the requirements under the DPA is entitled to compensation from the data controller for that damage. Additionally, an individual who suffers distress by reason of any contravention by a data controller of any of the requirements under the DPA is entitled to compensation, from the data controller, for that distress if:

- the individual also suffers damage by reason of the contravention; or
- the contravention relates to the processing of personal data for the special purposes.

Appeal Process

Any person aggrieved by a decision of the Information Commissioner, other than a decision in respect of an enforcement notice, assessment notice or information notice, may appeal to the Appeal Tribunal in accordance with such procedure as may be prescribed under the DPA. The appeal process has not yet been prescribed by the relevant Minister.

1.9 Enforcement Trends

The most significant privacy trend in the last 24 months was the public campaign which was launched by the Information Commissioner requiring the registration of data controllers with the Information Commissioner. The Information Commissioner embarked on a major campaign over the past two years encouraging data controllers to register and advising of the potential risks for failure to do so. Note, however, that to date, the Information Commissioner has not taken any enforcement action against a data controller for failure to register.

The practical takeaway for organisations is that failure to register with the Information Commissioner would constitute an offence under the DPA which could result in severe fines and penalties. Consequently, organisations must cease any further processing of

personal data unless and until they have registered with the Information Commissioner.

2. Privacy Litigation

2.1 Privacy Litigation Overview

In Jamaica, as the DPA was only recently enacted, privacy litigation is in its infancy.

As mentioned in **1.8 Enforcement Proceedings and Fines**, a claimant can bring a claim before the courts if he/she can prove that he/she has suffered some sort of damage due to any contravention by a data controller of any of the requirements under the DPA. The remedies available would be:

- compensation (damages);
- injunctions (including interim injunctions restraining further processing); and
- declaratory relief.

Additionally, an individual who suffers distress (ie, non-material damages) by reason of any contravention by a data controller of any of the requirements under the DPA can bring a claim before the courts for that distress if:

- the individual also suffers damage by reason of the contravention; or
- the contravention relates to the processing of personal data for so-called “special purposes” (such as journalism, art or literature).

Distress alone is not generally compensable and is recoverable only if:

- the claimant also suffered material “damage”; or
- the contravention relates to the “special purposes” (such as journalism, art or literature).

2.2 Recent Case Law

Morrison v Elephant Group Ltd (t/a Centerfield Jamaica) & others is one of the first reported Supreme Court decisions on the DPA regarding injunctive relief and the lawful bases for processing in an employment context.

In this decision, the claimant alleged that her employer's disclosure and dissemination of her personal data to a third-party company for the purposes of conducting background checks was unlawful and in breach of the DPA. The Supreme Court ruled that the employer's processing of personal data for background checks was permissible under the DPA. The decision pointed out that the DPA allows for the processing of personal data in certain circumstances, which include confidential background checks related to prospective employment.

Note that privacy litigation is not yet common in Jamaica.

2.3 Collective Redress Mechanisms

The DPA is silent with respect to collective redress. We do not have legislation in Jamaica which specifically governs collective redress.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

We do not have laws and/or regulations in Jamaica relating to the protection and processing of non-personal data. We are not aware of any plans by the government to enact laws similar to the EU Data Act in the near future.

3.2 Interaction of Data Regulation and Data Protection

Not applicable in this jurisdiction.

3.3 Rights and Obligations Under Applicable Data Regulation

Not applicable in this jurisdiction.

3.4 Regulators and Enforcement

Not applicable in this jurisdiction.

4. Sectoral Topics

4.1 Use of Cookies

Jamaica does not have a specific statute which governs cookies, SDKs and other device identifiers. Such

identifiers would be governed indirectly by the DPA once they can be used to personally identify an individual.

In practice, the following are usually treated as personal data:

- IP addresses;
- mobile advertising IDs;
- persistent cookies and SDK identifiers;
- device fingerprints; and
- analytics or ad IDs tied to accounts, profiles or behavioural patterns.

In Jamaica, online tracking is legal only insofar as it complies with general data protection principles. Note, however, that unfair or excessive tracking would be unlawful, and consent is effectively required for most advertising and cross-platform tracking technologies.

4.2 Personalised Advertising and Other Online Marketing Practices

Under the DPA, a data subject has the right to prevent processing of his/her personal data for direct marketing purposes unless the data subject gives his/her consent and/or is an existing customer of the data controller. This rule would also apply to sensitive or children's data.

Where consent is relied on, it must be:

- freely given;
- specific;
- informed; and
- unambiguous.

Where sensitive data is involved (eg, health, biometrics), consent must also be explicit and in writing.

4.3 Employment Privacy Law

In Jamaica, the privacy rights of employees are governed by the DPA along with general privacy principles and existing employment law. While the DPA does not include employment-specific provisions, its standards and individual rights apply broadly to employee-related data processing, including recruitment, monitoring, remote work arrangements, IT/BYOD policies,

background checks and the ongoing processing of personnel information.

When processing employee data, employers must ensure that the data is processed in accordance with the eight data protection principles as outlined under the DPA. These principles are as follows:

- *Fairness and lawfulness*: Employers may monitor employee activities (time tracking, system use, security monitoring) only in circumstances where it is necessary and justified, and employees must be informed of this monitoring. Monitoring must not be excessive, continuous or intrusive.
- *Purpose limitation*: Processing of employees' data must be limited to employment-related purposes.
- *Data minimisation*: Employers may collect personal data from prospective applicants but only what is necessary for recruiting or assessing suitability (eg, CV details, contact info, background checks).
- *Accuracy*: Employers should collect only data necessary for HR, payroll, benefits and legal compliance, and keep it accurate and up to date.
- *Storage limitation*: Employees' data must not be held for longer than needed, and employers are encouraged to implement retention policies which are to be shared with employee.
- *Rights of data subject*: Personal data must be processed in accordance with the rights of the employees.
- *Implementation of technical and organisational measures*: Employers should implement BYOD policies, IT policies and remote work arrangements which should be incorporated in the workplace.
- *Cross-border transfers*: Personal data of employees must not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of employees.

4.4 Data Protection in M&A

The DPA does not have specific provisions which govern M&A and asset deals in Jamaica. The general privacy principles as set out under the DPA would be applicable.

Due Diligence

With respect to due diligence, the acquiring entity should ensure that the target company is compliant with its legal obligations under the DPA such as registration with the Information Commissioner and appointment of a DPO. The acquiring entity should ensure that the target company has implemented certain policies to ensure compliance with the DPA, which include but are not limited to privacy policy, incident response policy, retention policy and BYOD policy. Lastly, the acquiring entity should ensure that the target company has implemented certain technical and organisational measures to prevent unauthorised access and/or disclosure of personal data such as access controls, VPNs, anti-virus software and security cameras.

Change of Control

The DPA requires data controllers to register with and notify the Information Commissioner of their processing activities. This includes providing organisational details and notifying it of changes such as a change of control of the data controller.

Notifications

Under the DPA, data controllers are required to be transparent about processing and provide privacy notices to data subjects. In the event that the acquiring entity intends to process personal data for new purposes beyond those originally disclosed by the target company, updated notices may need to be issued and fresh consent obtained where consent was the original basis.

Post-Closing Integration

After closing, the acquiring entity typically must:

- update privacy notices and public disclosures to reflect the new data controller's identity and purposes;
- align data inventories and processing records across the combined organisation; and
- ensure ongoing compliance with the DPA.

5. International Considerations

5.1 Restrictions on International Data Transfers

The DPA stipulates that personal data must not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The DPA further stipulates that with respect to cross-border transfers, the data controller must take into account the following:

- the nature of the personal data;
- the State or territory of origin of the information contained in the personal data;
- the State or territory of final destination of that information;
- the purposes for which and the period during which the personal data is intended to be processed;
- the law in force in the State or territory in question;
- the international obligations of that State or territory;
- any relevant codes of conduct or other rules which are enforceable in that State or territory (whether generally or by arrangement in particular cases); and
- any security measures taken in respect of the personal data in that State or territory.

The restrictions on cross-border transfers do not apply in the following circumstances:

- the data subject consents to the transfer;
- the transfer is necessary:
 - (a) for the performance of a contract between the data subject and the data controller; or
 - (b) for the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller;
- the transfer is necessary for the conclusion or performance of a contract, between the data controller and a person other than the data subject, which:
 - (a) is entered into at the request of the data subject;
 - (b) is in the interests of the data subject;

- the transfer is necessary for reasons of substantial public interest;
- the transfer;
 - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (b) is necessary for the purpose of obtaining legal advice; or
 - (c) is otherwise necessary for the purpose of establishing, exercising or defending legal rights;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the personal data is or may be disclosed after the transfer;
- the transfer is made on terms (which may include contractual terms) that are of a kind approved by the Information Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects;
- the transfer has been authorised by the Information Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects; or
- the transfer is necessary for the purposes of national security or the prevention, detection or investigation of crime.

5.2 Government Notifications and Approvals

There are no registrations, filings or approvals from authorities required for international transfers.

5.3 Data Localisation Requirements

There are no data localisation or residency obligations by sector or data category.

5.4 Blocking Statutes

No blocking or foreign-judgment control rules restrict foreign discovery, sanctions compliance or cross-border disclosures.

5.5 Recent Developments

There have not been any recent developments in the regulation of the international transfer of personal data.

Trends and Developments

Contributed by:

Marc Ramsay, Samantha Moore and Chantelle Biersay
Ramsay & Partners

Ramsay & Partners is a full-service law firm comprising six lawyers with a dedicated data protection and cybersecurity practice, led by a partner and supported by corporate, regulatory, employment and technology specialists. The firm is headquartered in Kingston, Jamaica, and is the exclusive member for Jamaica of the Chambers Band 1-ranked TerraLex global legal network, enabling structured multi-jurisdictional co-ordination across the Caribbean and key international markets. The practice advises on compliance with the Jamaica Data Protection Act, privacy governance, cybersecurity incident response, cross-

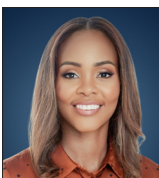
border data transfers, and data protection issues arising in corporate transactions, employment structures, fintech and regulated industries. Its work frequently intersects with governance, regulatory compliance and risk management. Recent matters include advising multinational technology companies on Jamaican data protection compliance and breach response, co-ordinating regional advice for cross-border operations, supporting financial services providers with data governance frameworks, and advising employers and healthcare-related entities on lawful processing, retention and regulatory engagement.

Authors



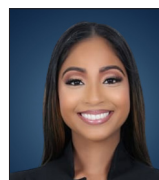
Marc Ramsay is the managing partner of Ramsay & Partners and supports the firm's data protection and cybersecurity practice through his work in governance, regulatory and compliance advisory. He advises

boards, regulators and senior management on organisational accountability, risk oversight and compliance structures, including where data protection obligations intersect with corporate governance, financial services regulation and cross-border operations. His experience includes advising on regulatory engagement, internal control frameworks and compliance risk allocation for technology-enabled and regulated businesses. Marc is admitted to practice in Jamaica, Belize and Barbados. He is a member of the Jamaican Bar Association and is a Professionally Accredited Company Secretary, with longstanding experience advising boards on governance and regulatory compliance matters.



Samantha Moore is a partner at Ramsay & Partners and leads the firm's data protection and cybersecurity practice. She advises on compliance with the Jamaica Data

Protection Act and related regulatory frameworks, including cross-border data protection issues and cybersecurity incident response. Her experience includes advising some of the world's largest technology companies as they navigate data protection obligations in Jamaica, including regulatory engagement and data breach response. She was called to the Jamaican Bar in December 2012 and joined the partnership in December 2020, having previously practised at a major Caribbean firm. Samantha is a member of the Jamaican Bar Association and serves on its Commercial Law and Telecommunications, Broadcasting & Technology subcommittees.



Chantelle Biersay is an associate at Ramsay & Partners and supports the firm's data protection and cybersecurity practice alongside her corporate and commercial work. She assists on data protection compliance

matters, including regulatory analysis, policy implementation, and advisory work where data protection issues arise in commercial transactions and operational structures. Her broader experience includes corporate transactions, real estate, conveyancing and capital markets work, including

high-value secured facilities for financial institutions. Chantelle was admitted to practice in Jamaica in 2020 and New York in 2025. She holds a Master of Laws in Corporate and Commercial Law and is a member of the Jamaican Bar Association.

Ramsay & Partners

8 Lady Musgrave Road,
Kingston 5,
St Andrew,
Jamaica

Tel: +1 876 906 2616
Email: inbox@ramsayandpartners.com
Web: jamaicadataprotection.com



RAMSAY & PARTNERS

Generative AI in Court Proceedings: Navigating the New Practice Direction

Key points:

- Jamaican courts now formally regulate how lawyers may use generative artificial intelligence in court matters.
- Lawyers remain fully responsible for everything filed in court, even if AI tools are used.
- AI cannot be used to create evidence, witness statements, affidavits or expert reports.
- Any use of AI in court documents must be disclosed to the court in a formal declaration.
- Failure to comply can result in documents being rejected, penalties or disciplinary action.
- Courts will not excuse mistakes caused by reliance on AI tools.
- AI may assist with drafting and efficiency, but only under strict conditions of verification and transparency.

Introduction

On 17 September 2025, the Honourable Chief Justice issued Practice Direction No. 1 of 2025 – Use of Generative Artificial Intelligence in Court Proceedings. This is the first formal statement by the judiciary of Jamaica on the permissible use of generative artificial intelligence (GenAI) in litigation. Its significance extends beyond attorneys alone. Clients who engage

legal counsel are directly affected, as the manner in which legal documents are prepared, verified, and presented to the Court now carries explicit regulatory consequences.

The Practice Direction applies across the Supreme Court of Judicature, the Revenue Court and both divisions of the Gun Court, and it has immediate implications for how legal services are delivered and supervised. It addresses growing concerns about accuracy, accountability and transparency amid the growing adoption of AI tools. The timing is notable. Ramsay & Partners recently encountered a matter in which opposing counsel relied on GenAI, resulting in fabricated cases, distorted formatting, unnatural language and stray special characters. At the time, the firm elected not to escalate the issue, given that no formal judicial guidance yet existed.

For clients, this development underscores an important reality. While technology may assist efficiency, responsibility for legal accuracy and integrity remains firmly with the attorney. The Practice Direction makes clear that courts will still look to counsel, not software.

Permitted use and continuing professional responsibility

The Practice Direction acknowledges the growing role of GenAI in drafting legal documents, research

and correspondence, but it sets strict conditions on how these tools may be used. Attorneys remain fully accountable for the contents of all documents filed. Any submission prepared with GenAI, whether in part or in whole, must be independently verified for factual accuracy and legal soundness. The Court makes it clear that responsibility cannot be shifted to technology. The duty of candour and diligence continues to rest with counsel, regardless of the sophistication of the tool employed.

Prohibited uses and protection of evidence integrity

Certain uses of GenAI are expressly prohibited. Attorneys may not rely on it to draft affidavits, witness statements or expert reports. Nor may it be used to generate or alter evidence, or to produce fabricated case law, statutory provisions or legal principles. The creation of avatars, images or likenesses for participation in virtual hearings is also forbidden. The scope of these restrictions makes plain the Court's intention to preserve the authenticity of evidence and the integrity of testimony.

Judicial scrutiny and evidentiary standards

The Practice Direction also introduces a formal disclosure obligation. Where any portion of a court document is prepared with the assistance of GenAI, the filing party must submit a declaration in the prescribed form. This declaration identifies the tool used and confirms that all citations and representations have been independently verified. Attorneys should treat this requirement with the same seriousness as the signing of pleadings or affidavits, since failure to comply may lead to documents being struck out, costs sanctions, contempt proceedings, or referral to the Disciplinary Committee of the General Legal Council. In less than obvious cases, determining whether an attorney has failed to disclose the use of GenAI will be difficult, as current AI detection tools such as GPTZero, Copyleaks and Turnitin may flag generative text, but their accuracy rarely exceeds 80% in practice, with paraphrasing or minor edits often defeating detection and false positives posing real risks in legal writing.

Judicial officers will assess AI-assisted submissions strictly against the same evidentiary and procedural rules that apply to all filings. The Court has made clear

it will not adjust or relax these standards to accommodate the use of new technology. This position signals caution: while the judiciary permits the use of GenAI, it will not extend any indulgence if the material contains errors, fabricated authorities or other defects. Attorneys must therefore treat every AI-assisted document as though it will be scrutinised with no margin for error, exactly as if it had been drafted entirely without technological support.

Practical uncertainties and emerging distinctions between tools

The framework is both enabling and cautionary. On the one hand, it confirms that the use of GenAI is permissible in Jamaican courts. On the other, it highlights risks that demand further thought from the profession. The prohibition on uploading confidential or privileged information to unsecured platforms is straightforward, yet the status of enterprise-grade or closed-system AI solutions remains uncertain. While the requirement to declare the use of GenAI is unambiguous, the extent of disclosure when tools are used merely for stylistic refinement, as opposed to substantive drafting, is less clear. For example, the use of unpaid general-purpose foundation models (LLMs) such as ChatGPT and Gemini is vastly different from paid models. Furthermore, the use of LLMs differs significantly from that of domain-specific applications, such as Vincent by vLex, Lexis+ AI, Harvey or the more familiar tool Grammarly. It is likely that attorneys who can disclose the use of credible, source-grounded, specialised legal GenAI tools will have an advantage, practically and perceived.

Recommended safeguards for practitioners

For practitioners, the prudent course is to implement internal safeguards. Every output from GenAI should be reviewed against primary sources and verified for accuracy. Confidential data should never be processed through unsecured systems. A clear justification record should be maintained, documenting why GenAI was used, how accuracy was confirmed and what protective measures were applied. Above all, attorneys must remember that the Court expects strict adherence to the Practice Direction rather than a creative interpretation.

Conclusion

This development does not close the door on the use of GenAI in litigation. Ramsay & Partners, for example, had adopted a formal AI governance policy tailored to comply with this Practice Direction. Rather than close the door to GenAI, it draws the boundaries within which responsible use is permitted. Attorneys can continue to benefit from efficiency and drafting support, provided they declare their use of the technology, ensure independent verification and maintain full professional accountability.



Law and Practice

Contributed by:

Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii
Mori Hamada & Matsumoto

Contents

1. Legal and Regulatory Framework p.239

- 1.1 Overview of Data and Privacy-Related Laws p.239
- 1.2 Rights and Obligations p.241
- 1.3 Special Categories of Personal Data p.244
- 1.4 Processing of Personal Data for Research and Development Purposes p.244
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.246
- 1.6 Data Breach Requirement p.246
- 1.7 Regulators p.247
- 1.8 Enforcement Proceedings and Fines p.248
- 1.9 Enforcement Trends p.248

2. Privacy Litigation p.248

- 2.1 Privacy Litigation Overview p.248
- 2.2 Recent Case Law p.248
- 2.3 Collective Redress Mechanisms p.249

3. Requirements for the Protection and Processing of Non-Personal Data p.249

- 3.1 Objectives and Scope of Data Regulation p.249
- 3.2 Interaction of Data Regulation and Data Protection p.249
- 3.3 Rights and Obligations Under Applicable Data Regulation p.249
- 3.4 Regulators and Enforcement p.249

4. Sectoral Topics p.249

- 4.1 Use of Cookies p.249
- 4.2 Personalised Advertising and Other Online Marketing Practices p.250
- 4.3 Employment Privacy Law p.250
- 4.4 Data Protection in M&A p.251

5. International Considerations p.251

- 5.1 Restrictions on International Data Transfers p.251
- 5.2 Government Notifications and Approvals p.252
- 5.3 Data Localisation Requirements p.252
- 5.4 Blocking Statutes p.252
- 5.5 Recent Developments p.252

Mori Hamada & Matsumoto is a full-service law firm that has served clients with distinction since its establishment in December 2002. The firm has experienced lawyers with considerable expertise in the constantly evolving and increasingly complex areas of information technology, life sciences and intellectual property, providing a variety of legal services in response to the diverse legal needs of its clients. These legal services include advising on regulatory requirements,

business set-up, corporate housekeeping, contract negotiations and dispute resolution. In terms of data protection, the firm has noted expertise in leveraging user information while protecting clients' businesses. Mori Hamada's data protection team comprises approximately 150 lawyers in our Tokyo, Osaka, Nagoya, Fukuoka, Beijing, Singapore, Manila and New York offices.

Authors



Yoshifumi Onodera is a senior partner at Mori Hamada, admitted to practise in Japan (Daini Tokyo Bar Association). Highly experienced in all data-related matters involving communication, media, competition,

consumer and/or information law, he is particularly adept at delivering advice to both foreign and domestic clients on complex business structures spanning vast content- and communication-related industries, including internet-related services, social networking services, games, music, movies and telecommunications. His expertise also extends to IP-related transactions concerning licensing and dispute resolution aspects in the subsidiary fields of infringement litigation, invalidity trials, appellate litigation and arbitration, and licensing in relation to intellectual property, including patents, trade marks and copyright.



Hiroyuki Tanaka is a partner at Mori Hamada, admitted to practise in Japan (Daini Tokyo Bar Association) and New York. His practice areas are data protection, IT and IP, and he has substantial experience advising

foreign clients on Japanese data protection law. Hiroyuki is also familiar with global data protection regulations, including the GDPR and CCPA, and helps Japanese clients with global data protection compliance by working closely with local counsels. He also advises on legal issues relating to AI (especially generative AI) and the protection of cybernetic avatars. Hiroyuki is an adjunct project professor at Keio University Graduate School of Law (2023–present).



Naoto Shimamura is a counsel at Mori Hamada, licensed in Japan (Daini Tokyo Bar Association), California and New York, and a lecturer at Ochanomizu University and Japan Women's University. He uses

his in-depth knowledge of computers and the internet to engage in technology-related cases, including those involving e-commerce, consumer protection, licensing, privacy, data protection, cybersecurity, online defamation, intellectual property and dispute resolution. Naoto is also qualified as a Certified Information Privacy Professional/Europe (CIPP/E), a Certified Information Privacy Professional/United States (CIPP/US), and a Registered Information Security Specialist, which is recognised as the highest level of security engineering qualification in Japan.



Rio Ichii is a junior associate at Mori Hamada, licensed in Japan (Daiichi Tokyo Bar Association). She has a broad portfolio and a wealth of experience across a number of practice areas, including IT, intellectual property, healthcare and trade law. She has also written many articles on these topics.

Mori Hamada & Matsumoto

16th Floor, Marunouchi Park Building
2-6-1 Marunouchi
Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6212 8330
Fax: +81 3 6212 8230
Email: info@morihamada.com
Web: www.morihamada.com

MORI HAMADA

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Japan's principal data protection legislation is the Act on the Protection of Personal Information (APPI). It provides the basic principles for the government's regulatory policies and authority, as well as the obligations of private business operators that handle personal information (handling operators).

Before April 2022, national administrative bodies were regulated by the Act on the Protection of Personal Information Held by Administrative Organs and the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc. However, thereafter, the obligations prescribed in these two laws were integrated into the APPI.

In addition, local government bodies are regulated under their own local regulations (*jourei*), but these vary between bodies. In April 2023, the APPI introduced nationwide principles for *jourei* and related implementation guidelines to homogenise the administration of national data protection regulations. Under this set of amendments, standard rules regarding personal information handled by local governments are uniformly stipulated in the APPI, while *jourei* can only stipulate local rules in very limited situations allowed under the law.

Where a personal information handling business operator located outside Japan handles personal information outside Japan relating to individuals located in

Japan in connection with the provision of goods or services to those persons, such handling is subject to the extraterritorial application of the APPI (Article 171).

For example, where a personal information handling business operator located outside Japan processes personal data outside Japan relating to users located in Japan pursuant to an outsourcing arrangement with a local business operator for the development and operation of an application intended for users in Japan, such processing by the foreign operator is considered to be in connection with the provision of goods or services to persons located in Japan and therefore falls within the scope of the extraterritorial application of the APPI.

In addition, as a general rule, personal information handling business operators located in Japan that provide personal data to personal information handling business operators located outside Japan are required to obtain the prior consent of the data subjects to the effect that the provision of personal data to third parties located outside Japan is permitted (Article 28.1).

Handling operators not limited to critical infrastructure must take necessary and appropriate action for security control over the personal data they handle, including preventing the leakage, loss or damage of or to personal data (Article 23).

Another important law is the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (the "My Number Act"), which stipulates

special rules for what is known in Japan as the Number to Identify a Specific Individual in Administrative Procedures (“My Number”), a 12-digit individual number assigned to each resident of Japan.

In June 2023, the Telecommunications Business Act (TBA) introduced a regulation about sending cookies to external parties. It also imposed new obligations regarding user information on large telecommunications service providers (TSPs) that have either 5 million paid users or 10 million free users.

Furthermore, the Personal Information Protection Commission (PPC – the regulator primarily responsible for the APPI and the My Number Act) has published guidelines for handling personal information (the “PPC Guidelines”). For some industrial sectors, the ministries with jurisdiction over them have published data protection guidelines for those sectors. For example, the Financial Services Agency (FSA) and the PPC have jointly published data protection guidelines for the financial sector, and the Ministry of Internal Affairs and Communications (MIC) has issued data protection guidelines for telecommunications business operators.

The APPI follows the Organisation for Economic Co-operation and Development’s eight Privacy Principles. Japan has reached an agreement with both the EU and the UK to certify each other’s country or territory as an “adequate” country for Japan’s and the EU/UK’s data protection purposes; this decision was renewed in March and April 2023. However, this does not mean that the APPI is identical to Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR).

Japanese data protection law is, nonetheless, closer to the EU omnibus model than the US sectoral/sub-national approach in the sense that Japan has a comprehensive data protection law: the APPI.

Draft Policy Outlining Reforms

On 9 January 2026, a draft policy outlining institutional reforms was released. The draft identifies four overarching themes:

- promotion of appropriate data utilisation;
- regulation appropriately tailored to risk;

- prevention of improper use and other misconduct; and
- measures to ensure the effectiveness of regulatory compliance.

The specific policy proposals under each theme are as follows.

Promotion of appropriate data utilisation

- With respect to the provision of personal data to third parties and the acquisition of publicly available sensitive personal information, consent of the data subject will not be required where such data is used solely for the creation of statistical information or similar purposes.
- Regarding regulations on use beyond the specified purpose, acquisition of sensitive personal information, and provision to third parties:
 - (a) consent of the data subject will not be required where, in light of the circumstances of acquisition, it is clear that the handling does not run counter to the data subject’s intent and does not harm the rights or interests of the data subject;
 - (b) the requirement that obtaining consent be difficult will be relaxed for cases where personal data is handled for the protection of life, body or property, or for the improvement of public health; and
 - (c) it will be expressly clarified that institutions or organisations whose purpose is the provision of medical care are included within the scope of “academic research institutions” eligible for the academic research exception.

Regulation appropriately tailored to risk

- Where the data subject is under 16 years of age, it will be explicitly stipulated that consent acquisition, notifications and similar procedures shall be directed to the legal guardian of the data subject. In addition, the requirements for requests to suspend the use of retained personal data relating to such minors will be relaxed, and a duty provision will be introduced requiring that the handling of minors’ personal information give priority to the best interests of the minor.
- With respect to facial feature data and similar information:

- (a) obligations will be imposed to publish certain matters relating to its handling;
- (b) the requirements for requests for suspension of use will be relaxed; and
- (c) provision to third parties based on the opt-out scheme will be prohibited.
- For businesses entrusted with data processing and similar services, the obligations concerning the appropriate handling of entrusted personal data will be reviewed.
- In the event of a data breach or similar incident, where there is little risk of harm to the rights or interests of the data subject, the obligation to notify the data subject will be relaxed.

Prevention of improper use and other misconduct

- With respect to information that does not constitute personal information but enables targeted approaches to specific individuals, improper use and unlawful acquisition of such information will be prohibited.
- For systems that permit provision of personal data to third parties without consent subject to certain conditions (opt-out schemes), obligations will be imposed to verify the identity of the recipient and the purpose of use.

Measures to ensure the effectiveness of regulatory compliance

- The requirements for issuing orders will be reviewed to enable more prompt correction of violations. In addition, recommendations or orders may be issued requiring measures necessary to protect the rights or interests of data subjects, such as notification to or public disclosure for affected individuals regarding the facts of the violation.
- A statutory basis will be established for requesting third parties who assist or facilitate violations to take necessary measures to cease such violations.
- With respect to penalties for the unlawful provision of personal information databases, acts of provision carried out for the purpose of causing harm will also be subject to punishment, and statutory penalties will be increased. In addition, penalties will be introduced for acts of unlawfully acquiring personal information through fraud or similar means.

- In order to effectively deter egregious violations involving the handling of large volumes of personal information driven by economic incentives, administrative fines will be introduced whereby, in cases of serious violations that infringe upon the rights or interests of individuals, payment of surcharges equivalent to the economic benefits obtained through the violation may be ordered.

1.2 Rights and Obligations

Handling Operator Duties

The obligations of handling operators under the APPI are as follows.

- They must specify and make known to data subjects the purpose of collecting their personal information (Articles 17 and 21).
- When a handling operator changes the purpose of use beyond what can be reasonably recognised as having relevance to the original purpose of use, the data subjects' consent is required (Articles 17.2 and 18.1). Exceptions to this consent requirement include instances when the use of information is required by law or is necessary to perform governmental duties, to protect the life, body or property of a person, or to improve public health (Article 18.3). Handling operators must not utilise personal information in a way that possibly foments or prompts unlawful or unfair acts (Article 19).
- When a handling operator obtains personal information of a person directly from documents (including electronic records) provided by that person, it must explicitly inform that person of the purpose of use in advance (Article 21.2).
- They must establish appropriate safeguards to protect personal data (Article 23).
- They must report data breach incidents to the PPC and notify affected data subjects in cases where their rights or interests are likely to be infringed (Article 26).
- They may not transfer personal data to another entity without the opt-in consent of the data subjects, unless they meet the requirements of any of the exceptions provided by the APPI (Article 27.1). These exceptions include instances where a transfer is required by law or is necessary to perform governmental duties to protect the life, body or property of a person or to improve public

health or is necessary for academic or research purposes (Article 27.1 (i)–(vii)). Other major exceptions include cases of entrustment of the handling of personal data to another entity, joint use of personal data with another entity, business succession resulting from a merger or other legal reasons (Article 27.5), or the filing of a notification of opt-out consent with the PPC (Article 27.2).

- They may not transfer personal data to countries that do not have sufficient data protection safeguards without the data subjects' consent (Article 28).
- They must keep records of the provision of personal data to third parties (Article 29).
- Upon receiving personal data from other handling operators, they must confirm the providing handling operator's compliance with applicable regulations regarding the provision of personal data and keep a record of the confirmation process (Article 30).
- They must handle pseudonymously and anonymously processed information in certain ways (Articles 41 to 46).

Entrustment

Under Article 27.5 (i) of the APPI, if a handling operator entrusts all or part of the handling of personal data it acquires to an individual or another entity, that individual or entity will not be considered a third party under Article 27.1. For example, if a handling operator uses third-party vendors of handling operator services and shares personal data with those vendors for them to use on the handling operator's behalf and not for their own use, that transfer will be deemed an "entrustment" and is not subject to data transfer restrictions.

When a handling operator "entrusts" personal data, it must exercise appropriate supervision as necessary over the entrusted person to ensure security control over the entrusted personal data (Article 25).

Joint Use

Handling operators may share and jointly use personal data with specific individuals or entities as long as the handling operator notifies the data subjects or makes the following information accessible to them (Article 27.5 (iii)) before any information sharing or joint use:

- the fact that personal data will be used jointly with specific individuals or entities;
- the personal data to be used jointly;
- who the joint users are;
- the purpose of the joint use; and
- the name of the individual or entity responsible for managing the personal data (the address of the responsible individual or entity and, if it is a corporate body, the name of its representative are also required).

After this information is published or the data subjects are notified of the same, the identified joint users will not be deemed third parties within the context of Article 27 and, therefore, the handling operator and the identified joint users may share and jointly use specific items of personal data as if they were a single entity.

Business Succession

Handling operators may transfer personal data to third parties without the opt-in consent of data subjects if the transfer accompanies a business succession caused by a merger or for other legal reason (Article 27.5 (ii)).

Filing of Notification of Opt-Out Consent

Under Article 27.2 of the APPI, handling operators may provide personal data (excluding special-care-required personal information and personal data acquired by improper means or provided by another handling operator pursuant to the opt-out mechanism) to third parties without the opt-in consent of data subjects if the following conditions are met:

- they agree to stop providing personal data to the third party upon the data subjects' demand;
- they notify the data subjects in advance of certain events outlined in Article 27.2 or make such notification of events readily accessible to the data subjects; and
- they submit a notification of certain matters to the PPC.

Please note that, in practice, the PPC does not readily accept the foregoing opt-out notification unless it is not practical to seek the data subjects' consent and it is difficult to use the other exceptions.

Data Protection Officers

The APPI has no provision mandating the appointment of privacy or data protection officers; however, handling operators must take necessary and proper measures to prevent the leakage, loss or damage of or to personal data and to implement other security controls. Under the PPC Guidelines, those measures should include the following:

- organisational security measures, such as establishing rules for handling personal data and clarifying who is responsible for supervising such handling;
- HR security measures, including educating/training employees;
- physical security measures, including controlling the areas where personal data is handled, such as servers and offices;
- technical security measures, including controlling access to personal data; and
- understanding of the external environment – this security measure, introduced in the amendments to the guidelines, requires handling operators that process personal data in foreign countries to understand the foreign country's legal system for personal information protection and, taking that legal system into consideration, to take necessary and appropriate measures to ensure the security of personal data.

Effective since April 2024, the PPC Guidelines also require handling operators to take security control over personal information that is collected and expected to be treated as personal data to prevent cyber-attackers from intercepting it on the operators' behalf.

The PPC Guidelines indicate the appointment of a person to be in charge of the handling of personal data as an example of a proper and necessary measure. However, although handling operators are expected to adopt the measures described in the PPC Guidelines, any failure to adopt such measures is not a direct breach of the APPI.

Under the TBA, large TSPs are required to appoint a chief manager responsible for handling user information.

Privacy By Design/Default and Privacy Impact Analyses (PIAs)

The APPI does not mandate obligations regarding PIAs. However, the PPC has issued a report titled "Promoting the implementation of PIAs – Significance of PIAs and points to keep in mind in the implementation process", which business operators are encouraged to follow voluntarily. The APPI does not refer to the concepts of privacy by design or default, but PPC guidelines on accredited personal information protection organisations recommend that these organisations promote privacy by design.

Internal or External Privacy Policy

The PPC Guidelines recommend releasing a privacy policy or statement.

Article 32.1 of the APPI requires handling operators to make the following information regarding retained personal data available to data subjects:

- the name of the handling operator, an address for the individual or entity responsible and, if it is a corporate body, the name of its representative;
- the purposes of use of retained personal data;
- the procedures for responding to requests from data subjects to disclose, correct, suspend the use of or erase retained personal data;
- contact information for accepting complaints regarding the processing of retained personal data; and
- security measures being implemented by the handling operator.

Most handling operators typically comply by using internal and external privacy policies.

The PPC Guidelines also recommend stating the following in a handling operator's basic policies as part of the implementation of security control measures regarding personal data:

- the name of the handling operator;
- compliance with relevant laws, regulations and guidelines;
- an explanation of security control measures regarding personal data; and
- contact details for complaints and questions.

Most handling operators typically comply by using internal and external privacy policies.

The PPC Guidelines also recommend being transparent in disclosing the entrustment of work involving personal data (eg, disclosing whether entrustment has been made and what kind of work has been entrusted).

Data Subjects' Rights

Data subjects may request handling operators to disclose their retained personal data and the record of its provision to third parties. Handling operators must comply with these requests unless there is a possibility that the disclosure could harm the data subject's or a third party's life, body, property or other rights or interests, or that it could seriously interfere with the handling operator's business (Article 33).

Data subjects may also request handling operators to correct, add or delete retained personal data. The handling operator must investigate without delay and, based on the results of the investigation, comply with these requests to the extent necessary to achieve the purposes of use of the retained personal data (Article 34).

Furthermore, data subjects may request that handling operators discontinue the use of or erase retained personal data and stop providing retained personal data to third parties if:

- the data was or is being acquired, processed or provided to a third party in violation of the APPI;
- the retention of retained personal data has become unnecessary;
- a data breach has occurred regarding the retained personal data; or
- there is a possibility that the handling of the retained personal data would harm the rights or legitimate interests of the data subjects.

However, this obligation will not apply if it will be too costly or difficult to discontinue the use of or erase the retained personal data and the handling operator takes necessary alternative measures to protect the rights and interests of the data subjects (Article 35).

1.3 Special Categories of Personal Data

"Special care-required personal information" refers to personal information that requires special care in its handling so as not to cause unfair discrimination, prejudice or other disadvantages to the individual, including information relating to a person's race, creed, social status, medical history, criminal record, or the fact of having been a victim of a crime.

The acquisition of special care-required personal information and the provision of such information to third parties require the prior consent of the data subject, and an opt-out mechanism is not available.

Where a leakage or other incident involving personal data containing sensitive personal information has occurred, or where there is a risk of such an incident occurring, the personal information handling business operator is required to report the incident to the PPC and notify the data subject.

1.4 Processing of Personal Data for Research and Development Purposes

APPI

The APPI recognises the concept of anonymously processed information, which is defined as information obtained by processing personal information such that ordinary people cannot identify a specific data subject using the processed information or restore any personal information from the processed information (Article 2.6). This framework intends to promote the use of anonymously processed information by clarifying the rules and was expected to lead to the use of big data, innovations and new businesses. Handling operators can provide anonymously processed information to third parties without the consent of the data subjects, provided that the handling operator:

- produces the anonymously processed information in compliance with the standards set forth in the PPC Ordinance (Article 43.1);
- takes measures for security control in compliance with the standards set forth in the PPC Ordinance to prevent leakage (Article 43.2);
- discloses information that will be included in the anonymously processed information pursuant to the PPC Ordinance (Article 43.3);

- when it provides anonymously processed information to third parties, discloses information that will be included in the anonymously processed information and the medium to be used to deliver the information in compliance with the PPC Ordinance, and explicitly informs the third-party recipients that the disclosed information is anonymously processed information (Article 43.4);
- does not do anything to identify the individual (Article 43.5); and
- takes measures to secure the safe control of, and address complaints regarding, the handling of anonymously processed information and to publicly announce such measures (Article 43.6).

According to the PPC Guidelines, statistical information, meaning information that can be obtained by extracting data concerning a common element from information taken from several people and tallying them up by category, is not anonymously processed information because statistical information is not information regarding an individual and, thus, is not covered by any regulations under the APPI.

The 2020 amendment of the APPI introduced the concept of pseudonymously processed information. This is information that is processed so that it cannot be used to identify a specific individual without collation with other information (Article 2.5). Pseudonymously processed information is exempted from certain regulations under the APPI, such as restrictions on changing the purpose of use and the obligation to comply with the data subject's rights, and report/notification obligations in the case of a data breach (Article 43).

Next-Generation Medical Infrastructure Act

In May 2023, the Next-Generation Medical Infrastructure Act was promulgated as a special act under the APPI, with the aim of promoting the use of anonymised individual medical information – such as health check-up results and medical records – for research and development in the medical field. The law establishes a new system for creating and using “pseudonymously processed medical information”.

“Pseudonymously processed medical information” refers to information that has been processed so that an individual cannot be identified unless it is collated

with other information. While it requires the removal of identifiers such as names and IDs from personal information, it does not require the removal of distinctive values or names of rare diseases.

The Next-Generation Medical Infrastructure Act is broadly composed of the following three elements.

Certification of businesses creating pseudonymously processed medical information

The government certifies businesses that receive medical information from medical institutions based on notification to the individuals concerned, and that create and provide pseudonymously processed medical information (“certified pseudonymously processed medical information creation businesses”).

Certification of users of pseudonymously processed medical information

Certified pseudonymously processed medical information creation businesses may provide pseudonymously processed medical information only to users certified by the government in accordance with standards such as security management (“certified pseudonymously processed medical information user businesses”).

Certified pseudonymously processed medical information user businesses are prohibited from re-identifying the information and from providing it to third parties. However, exceptions are permitted, such as submission to the Pharmaceuticals and Medical Devices Agency (PMDA), an incorporated administrative agency that conducts pharmaceutical approval reviews, and joint use among certified pseudonymously processed medical information user businesses.

Use of pseudonymously processed medical information to support pharmaceutical approval

For the purpose of applying for pharmaceutical approval, certified pseudonymously processed medical information user businesses are permitted to provide pseudonymously processed medical information to the PMDA and other relevant bodies.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Legal problems concerning AI have been the subject of intense discussion of late, including matters such as liability for the actions of AI and ownership of rights regarding AI-created content.

On 1 September 2025, the AI Act took effect, which addresses risks associated with AI while promoting innovation. It provides for the establishment of an AI Strategy Headquarters, headed by the Prime Minister and composed of other ministers, and sets forth the basic policies for measures to be implemented by the government to promote research, development and utilisation of AI. The law also defines fundamental measures relating to AI. The AI Act expresses the government's overall stance on AI-related matters and does not contain specific compliance obligations, requirements or penalty provisions.

The PPC published an announcement in June 2023 stating its interpretation of the APPI in the context of generative AI and requesting generative AI service providers and users to comply with the law. MIC and the Ministry of Economy, Trade and Industry (METI) published their AI Business Guidelines for AI developers, service providers and users in April 2024. These guidelines include cautions and points to note regarding privacy and data protection.

The Institute for Information and Communications Policy (IICP) and MIC have jointly published the Draft AI R&D Guidelines for International Discussions, which explain the R&D and nine other principles for research into and development of AI. These are tentative guidelines for further international discussion. MIC also published the Guidelines for AI Utilisation in August 2019, which summarise the issues that users (including service providers) are expected to pay attention to in their utilisation phase of AI in the form of "principles" and provide explanations based on the principle of a human-centred AI society. Some other AI-related associations have also published similar principles or guidelines for research into and development of artificial intelligence.

There are no regulations specific to AI data, but please note that general regulations are applicable.

For example, if AI data includes personal information, the APPI applies to the processing of that data.

1.6 Data Breach Requirement

According to the guidelines issued by the PPC, where a business operator handling personal information becomes aware of an actual or suspected data breach, it is required to take necessary measures with respect to the following matters, depending on the nature and circumstances of the incident.

- *Internal reporting and prevention of further damage* – The business operator must promptly report the incident to a person in a position of responsibility within the organisation and take necessary measures to prevent the damage caused by the leakage from spreading beyond what existed when the incident was discovered.
- *Investigation of the facts and identification of the cause* – The business operator must take necessary measures to investigate the facts surrounding the leakage and to identify its cause.
- *Identification of the scope of impact* – The business operator must take necessary measures to identify the scope of impact of the leakage.
- *Consideration and implementation of measures to prevent recurrence* – The business operator must take necessary measures to consider and implement measures to prevent recurrence of the leakage.

Further, business operators handling personal information must report to the PPC when they become aware of a data breach in any of the following circumstances (Article 26.1):

- where actual or suspected leakage involves personal data containing sensitive personal information (see **1.3 Special Categories of Personal Data**);
- where actual or suspected leakage involves personal data that is likely to result in financial harm if improperly used;
- where actual or suspected leakage results from an act directed at the business operator that is suspected to have been carried out for an unlawful purpose; or

- where actual or suspected leakage involves personal data relating to more than 1,000 data subjects.

The matters that must be reported to the PPC are as follows:

- (i) overview of the incident, including the date of occurrence, date of discovery, description of the incident, person who discovered it, the applicable reporting category, the existence of an outsourcing relationship (including the identity of the principal and contractor, if any), and the course of events;
- (ii) items, media and types of personal data involved in the actual or suspected leakage;
- (iii) number of data subjects whose personal data was involved;
- (iv) cause of the leakage and the responsible party;
- (v) existence and details of secondary damage, or the risk thereof;
- (vi) status of responses to the data subjects;
- (vii) status of public disclosure of the fact of the leakage;
- (viii) measures taken to prevent recurrence; and
- (ix) any other relevant information.

Business operators handling personal information are required to submit a preliminary report within three to five days after becoming aware of the above matters, and to file a final report within 30 days. However, in cases where actual or suspected leakage results from an act directed at the business operator that is suspected to have been carried out for an unlawful purpose, the final report must be submitted within 60 days. If it is difficult for the business operator to report all of the required items in the final report, it is allowed to report only identified items at that point and to supplement the remaining items as they are identified.

Business operators handling personal information must notify the data subjects of data breaches upon becoming aware of them with respect to items (i), (ii), (iv), (v) and (ix) above (Article 26.2 of the APPI).

According to the guidelines issued by the PPC, where a data breach has occurred, it is desirable to promptly

disclose information concerning the facts of the incident and the measures taken to prevent recurrence.

1.7 Regulators

The PPC is tasked with enforcing and implementing the APPI, and has the following powers:

- to require handling operators to report or submit materials regarding their handling of personal information; and to enter handling operators' offices or other locations to investigate, make enquiries and view records or other documents (Article 146);
- to provide guidance or advice to handling operators (Article 147);
- to recommend that handling operators cease any violations of the APPI and take other necessary measures to correct the violations (Article 148.1);
- to order handling operators to take necessary measures to implement the PPC's recommendations mentioned above and rectify certain violations of the APPI (Articles 148.2 and 148.3); and
- to publicly announce any handling operators' violations of orders issued by the PPC pursuant to Articles 148.2 and 148.3 (Article 148.4).

The PPC initiates investigations based on information obtained not only from reports submitted by business operators but also through requests for reports and on-site inspections. The PPC makes available on its website detailed guidelines concerning the APPI, which are commonly relied upon in interpreting the law, including the obligations imposed on business operators.

For some sectors, other government authorities also enforce the APPI – for example, the FSA is the relevant authority for banks, whereas MIC is the appropriate authority for TSPs. There are no regulators specifically overseeing AI data.

The PPC does not have the authority to conduct criminal investigations, and the APPI explicitly stipulates that the commission's power to conduct on-site inspections does not include criminal investigations (Article 146.3).

It is important to note that the APPI imposes no administrative fines. Criminal sanctions may only be imposed if a handling operator:

- refuses to co-operate with or makes any false report in response to an investigation by the PPC (Article 178);
- provides a personal information database to unauthorised persons or misuses the database for unlawful gains (Article 180); or
- violates any order given by the PPC as part of an administrative sanction (Article 181).

The PPC empowers private organisations called accredited personal information protection organisations (*nintei kojīn jōuhō hōgō dantai*) to handle and promote the protection of the personal information held by handling operators. These accredited organisations process complaints against handling operators or provide information on them to ensure the reliability of the businesses of those handling operators, and promote the protection of personal information. They also establish their own rules, with which their members must comply.

1.8 Enforcement Proceedings and Fines

The PPC finds potential violations of the APPI through data breach reports submitted by handling operators, telephone consultations made through their business support desk, and media coverage. Please see **1.7 Regulators** for details.

The PPC has the power to enforce administrative sanctions, but the APPI does not provide for administrative fines; please see **1.7 Regulators** for details. Introduction of administrative fines is under discussion; please refer to **1.1 Overview of Data and Privacy-Related Laws** for more details. The PPC provides guidance or advice and does not take further action in most cases, although it does take strong action such as issuing orders in serious cases.

1.9 Enforcement Trends

In June 2024, it was discovered that insurance agents handling products from multiple non-life insurance companies had, without obtaining the consent of policyholders, provided personal data of insurance policyholders (including names, policy numbers,

premiums, and the names of the insurers with which contracts were concluded) to other non-life insurance companies. In addition, employees seconded from non-life insurance companies to insurance agents were found to have, without authorisation from the host insurance agent and without the consent of the data subjects, transmitted personal data (including names, policy numbers, premiums, insurer names and policy periods) by email or other means to their insurance companies.

Following an investigation by the FSA, a business improvement order was issued on 24 March 2025. The PPC also issued administrative guidance on 30 April 2025. The authorities pointed out that the sharing of personal information among companies for the purpose of acquiring insurance contracts had become a common practice, and that there was a lack of organisation-wide awareness regarding the proper management of personal information. The case underscores the importance of prioritising legal compliance over business convenience or industry customs and maintaining a strong compliance-oriented mindset throughout the organisation.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Data subjects may go to court to seek compensation for damages or distress caused by breaches of data protection. There are two major types of legal causes.

- First, Japanese courts recognise the right to privacy, which is the right of persons not to have their private lives disclosed except for legitimate reasons. Breaching the right to privacy constitutes tort under Article 709 of the Civil Code.
- Second, if a business promises to keep personal data confidential in an agreement (such as terms of use) but then compromises the data, the legal cause of breach of contract may also be available.

2.2 Recent Case Law

In October 2017, the Supreme Court rendered a decision granting a claim for damages for the infringement of privacy in a case where a company providing correspondence education services for children was

sued for damages in tort. The case arose from a personal data breach caused by a former employee of a subcontractor responsible for the development and operation of the company's systems, who unlawfully removed a large volume of personal information relating to the company's customers from its database.

The Court held that even if there had been no allegation or proof that the plaintiffs had been harmed beyond mere discomfort or anxiety – such as being subjected to nuisance conduct or financial loss – as a result of the data breach, it was nevertheless necessary, in so far as the leakage resulted in an infringement of privacy, to examine whether the plaintiffs had suffered mental distress from the invasion of privacy itself, as well as the existence and extent of such distress.

2.3 Collective Redress Mechanisms

The Act on Special Measures Concerning Civil Court Proceedings for the Collective Redress for Property Damage Incurred by Consumers allows for class actions to be filed by consumers. Please note that claims allowed under the law are limited to property damage and emotional distress within the scope of the class action itself if the distress is caused along with property damage or by intentional conduct.

As a practical matter, multiple data subjects may select the same lawyer to represent them, and that lawyer can file a single lawsuit on their behalf, which is similar to a class action. There is no difference in the standards for court acceptance or the duration of proceedings compared with ordinary cases of a similar scale.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation Internet of Things (IoT) Services

Legal problems regarding the IoT and ubiquitous sensors have been the subject of intense discussion of late, but no specific laws or regulations are currently targeting either issue. However, MIC has published guidelines regarding comprehensive measures for IoT security (July 2016).

The Information-technology Promotion Agency introduced a security requirement compliance evaluation and labelling system for security features of IoT products (JC-STAR) in March 2025.

Big Data

As for big data analytics, data sharing will typically happen between companies subject to contracts between those companies. METI has published guidelines on contracts regarding sharing (big) data between companies. Big data may contain special care-required personal information, such as medical histories. Regarding regulation of special care-required personal information, see **1.3 Special Categories of Personal Data**.

Personal data that has been processed so as to render specific individuals unidentifiable does not constitute personal information under the APPI and may therefore be provided to third parties subject to certain conditions without consent.

3.2 Interaction of Data Regulation and Data Protection

See **3.1 Objectives and Scope of Data Regulation**.

3.3 Rights and Obligations Under Applicable Data Regulation

See **3.1 Objectives and Scope of Data Regulation**.

3.4 Regulators and Enforcement

See **1.7 Regulators** and **1.9 Enforcement Trends**.

4. Sectoral Topics

4.1 Use of Cookies

The use of cookies, web beacons and other tracking technology is not directly regulated under the APPI. Information collected by cookies or web beacons is not automatically deemed to be personal information, but it will be if the handling operator can easily collate information collected by cookies or web beacons with the names of individuals (for example, when an internet-based company can identify the cookie IDs of customers when logged in to its website).

In this regard, the transfer of personal data to third parties – whether the data is personal data or not – is determined based on the circumstances surrounding the transferor, not the transferee. In brief, if the data is not personal data in the hands of the transferor, regulations regarding the transfer of personal data to third parties are not applicable.

In the past, some schemes emerged whereby data management platforms provided non-personal information such as user data collected by cookies (eg, user browsing histories, interests, preferences) to third parties, with the knowledge that the data will be personal data in the hands of the recipient. The PPC was concerned by the expansion of this kind of data-sharing without the involvement of (control by) the data subjects.

As a result, the concept of personally referable information was introduced in April 2022, defined as a collective set of information comprising information relating to living individuals that does not fall under personal information or pseudonymously or anonymously processed information but that has been systematically organised to be searchable using a computer for specific personally referable or similar information prescribed by cabinet order. The APPI regulates the provision of personally referable information if the provider assumes that recipients will acquire a database of the provided personally referable information as personal data. In such cases, the transferor must confirm that the transferee has obtained the data subjects' consent to transfer their data as personal data.

Please also refer to **4.2 Personalised Advertising and Other Online Marketing Practices** for the TBA regulation for technology to send information to external parties.

4.2 Personalised Advertising and Other Online Marketing Practices

Behavioural advertising is not directly regulated under the APPI, but any personal information collected to provide such advertising is subject to the law. For example, the APPI has regulations for certain cookies, web beacons and other tracking technology underlying behavioural or targeted advertising. Please

see **4.1 Use of Cookies**. It is good practice to have a cookie policy and to offer an opt-out from using cookies (especially for behavioural advertising). The Japan Interactive Advertising Association's guidelines are useful for gaining an understanding of good practices in Japan.

Effective since June 2023, the TBA imposed new obligations on TSPs, which have a non-trivial impact on users' interests. More specifically, a TSP is an entity that provides:

- any services of intermediating telecommunication of others, such as email or direct messaging services;
- social media services, bulletin board systems, movie sharing services, online shopping malls, live streaming services, online games, online education or the like;
- online search engines; or
- various information, such as news, weather, movies and maps, to unspecified people.

When a TSP makes users send their information (typically including cookies) to an external party, the TSP is required to make a notification or public announcement, obtain opt-in consent or provide an opt-out mechanism with respect to certain information, including the content of the information, the name of the recipient party and the recipient's purpose of use of the information.

4.3 Employment Privacy Law

The Ministry of Health, Labour and Welfare (MHLW) has issued a notice regarding the handling of health information of employees by employers, including a condition that the employer shall not handle such information beyond the scope necessary to secure its employees' health.

Furthermore, to prevent discrimination, the Employment Security Act has special restrictions on obtaining information about job applicants during their recruitment.

The employer has the right to monitor workplace communications in relation to work and to use cybersecurity tools, insider threat detection and prevention

programmes, and digital loss prevention technologies, but privacy issues may arise regarding private communications and other privacy matters at the workplace. Thus, employers are recommended to establish internal rules prohibiting the use of company PCs and email addresses for private use, and to disclose the possibility of monitoring those devices and data, including emails.

In principle, there is no special role for labour organisations or works councils regarding employment-related data privacy, but there is a general requirement for employers to obtain the opinion of the employee representative in establishing work rules.

4.4 Data Protection in M&A

The APPI has some special rules for data processing in relation to M&A. Where personal information is provided in connection with a business succession, it is not necessary to obtain the data subject's consent. See "Business Succession" under 1.2 Rights and Obligations.

Handling operators are required to specify the purpose of use when acquiring personal information (Article 27 (a)) and to notify the data subject of or publicly announce such purpose (Article 27 (5)(ii)). The operator may use personal information only to the extent necessary to achieve the specified purpose of use.

Where the target company and the buyer are integrated through a business succession, the personal information acquired prior to the integration is considered to have been obtained for different purposes based on the respective pre-integration privacy policies or similar documents of the target company and the buyer. Accordingly, such personal information may not be used, after the integration, for purposes that were not originally contemplated. Nor is it permissible to use personal information previously held for services newly created as a result of the business integration.

In such cases, the personal information handling business operator must either obtain the data subject's consent to change the purpose of use, or clearly classify and manage personal information by distinguishing between information acquired prior to and after the integration.

5. International Considerations

5.1 Restrictions on International Data Transfers

There are special restrictions on the transfer of personal data to foreign countries. In principle, the APPI requires the transferor to obtain the prior consent of individuals whose personal data will be transferred to third parties located in foreign countries (Article 28). Thus, overseas transfer restrictions will apply if a foreign company transfers user data to another company outside Japan. However, if it does so to a company in Japan, overseas transfer restrictions will not apply. These restrictions apply even in cases of entrustment and joint use, which are exceptions to local third-party data transfer restrictions.

Data subjects' consent to overseas data transfers is not necessary only if either of the following applies:

- the PPC designates the foreign country as a country with a data protection regime with a level of protection equivalent to that of Japan (only member countries of the EEA and the UK have been designated to date); or
- the third-party recipient has an equivalent system of data protection that meets the standards prescribed by the PPC Ordinance – ie, either of the following:
 - (a) there is assurance, by appropriate and reasonable methodologies, that the recipient will treat the disclosed personal data in accordance with the spirit of the requirements for handling personal data under the APPI; or
 - (b) the recipient has been certified under an international arrangement recognised by the PPC regarding its system of handling personal data.

Implementation of the PPC Ordinance is provided for in the PPC Guidelines, under which the "appropriate and reasonable methodologies" referred to above include agreements between the data importer and exporter, or intergroup privacy rules, which ensure that the data importer will treat the disclosed personal data in accordance with the spirit of the APPI. With respect to recognised international arrangements, the PPC Guidelines have identified the APEC Cross-Border

Privacy Rules (CBPR) as a recognised international framework for the handling of personal information.

Please also refer to **5.5 Recent Developments** for additional obligations effective since April 2022.

5.2 Government Notifications and Approvals

Overseas data transfer restrictions do not require government notification or approval.

5.3 Data Localisation Requirements

There are no data localisation requirements under the APPI.

5.4 Blocking Statutes

There are no blocking statutes under Japanese law.

5.5 Recent Developments

Effective since April 2022, international data transfers are permitted only when additional requirements are met. First, when handling operators transfer personal data to foreign countries based on the aforementioned consent mechanism, they will be required to provide data subjects with certain information, as specified by the amended ordinance issued by the PPC (the “Amended PPC Ordinance”) (Article 28.2). According to the PPC Ordinance, the foreign country’s name, information about its personal information protection system and the measures to be taken by the recipient party to protect personal information are required to be provided to the data subjects.

Second, when handling operators transfer personal data relying on the recipient’s equivalent system of data protection, they will be required to take the necessary steps to ensure that the overseas recipient continuously takes equivalent measures and to provide data subjects with certain information about the measures to be taken upon request under the Amended PPC

Ordinance (Article 28.3). In this regard, according to the PPC Ordinance, one of two assurance measures is to periodically confirm the implementation status of the equivalent measures taken by the recipient and the presence or absence of systems in the foreign country that might affect the implementation of the equivalent measures. The other measure is to take necessary and appropriate measures if the recipient party’s implementation of the equivalent measures is interfered with in some way, and to suspend the provision of personal data if it becomes difficult to ensure the continuous implementation of the equivalent measures.

The PPC Ordinance also states that the following information must be provided to data subjects upon request:

- the recipient party’s equivalent system of data protection;
- an outline of the equivalent measures taken by the recipient;
- the frequency and method of confirmation of the status of the equivalent measures and of the system in the foreign country that might affect the implementation of the measures;
- the name of the foreign country;
- the presence or absence of systems in that foreign country that might affect the implementation of the equivalent measures;
- the presence or absence of any impediments to the implementation of the equivalent measures; and
- an outline of the measures to be taken in response to such impediments.

As a result, data transfers to countries where proper government access is not implemented can be difficult. An example of this difficulty is the international data transfer regulations under the GDPR raised by the *Schrems II* case.

Trends and Developments

Contributed by:

Yuki Kuroda, Takuya Uehara and Nanoko Sasaki
Oh-Ebashi LPC & Partners

Oh-Ebashi LPC & Partners is a full-service law firm with over 160 attorneys, and its main offices are in Tokyo and Osaka. It was originally established in Osaka in 1981 but now has an equivalent-sized operation in Tokyo. It was the first Japanese law firm to open an office in China and, together with its Nagoya office, currently has offices in four locations. Its legal practice covers a broad range of fields, including

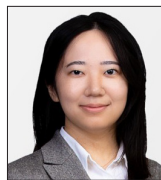
corporate/M&A, risk management and compliance, IP law, life sciences, restructuring/insolvency, competition and antitrust/consumer protection, dispute resolution, finance and insurance, employment law, administration/regulatory law and tax law. It also provides an international practice, a China/Asian practice, a private practice and a pro bono practice.

Authors



Yuki Kuroda is a partner at Oh-Ebashi LPC & Partners and is in charge of data protection and data security issues. He has handled a number of law and technology cases throughout his career. His practice includes

Japanese and international data protection cases, and he regularly guides clients on planning new data-intensive businesses and implementing robust data protection/security compliance programmes. He received a PhD degree from Kyoto University Graduate School of Informatics, an LLM degree from the University of California, Berkeley, and a J.D. degree from Osaka University. He is licensed to practise law in Japan and New York.



Nanoko Sasaki is an associate at Oh-Ebashi LPC & Partners, where her practice focuses on data protection and cybersecurity law, commercial litigation and general corporate practice. She has represented a

multinational corporation in cyber litigation matters, including a case regarding a sender identification information disclosure order. She has extensive experience in domestic and cross-border M&A, having played significant roles in numerous transactions. She received both a J.D. degree and a B.A. degree from the University of Tokyo, and is licensed to practise law in Japan.



Takuya Uehara is a partner at Oh-Ebashi LPC & Partners and advises various companies on technology-related matters, including how to operate systems for e-commerce and digital

advertisement. He has extensive experience in advising on how to comply with regulations on electronic data usage and protection, and substantial expertise in risk management and compliance, including how to respond to data security incidents. He received an LLM degree from the University of Pennsylvania and a J.D. degree from the University of Tokyo, and is licensed to practise law in Japan and New York.

Oh-Ebashi LPC & Partners

Kishimoto Building 2F
2-2-1 Marunouchi, Chiyoda-ku
Tokyo 100-0005
Japan

Tel: +81 3 5224 5566
Fax: +81 3 5224 5565
Email: general_toiawase@ohebashi.com
Web: www.ohebashi.com/en

OH-EBASHI

大江橋法律事務所

Introduction

The Act on the Protection of Personal Information (APPI) serves as Japan's fundamental and comprehensive data protection legislation.

When the APPI underwent significant amendments in 2020, it was stipulated that its provisions should be reviewed approximately every three years following the implementation of the amended law. Therefore, the Personal Information Protection Commission (PPC), which was established as the data protection authority under the APPI, initiated its review in November 2023 and published an Interim Report in June 2024.

Based on the results of hearings with experts and other stakeholders, the PPC examined and reassessed the institutional issues that were identified in the Interim Report, and began discussing such issues in January 2025. The issues were associated with three main topics:

- how to involve data subjects in the processing of their personal data;
- how to respond to risks arising out of diversifying ways to process personal data; and
- how to ensure the effectiveness of compliance by businesses processing personal data.

In March 2025, the PPC published its “Views on Institutional Issues”, a document summarising its discussions and its views on the institutional issues concerning the APPI. It then published its “Policy on Institutional Amendments” in January 2026, outlining the following four pillars of the APPI amendment:

- the promotion of proper data utilisation;
- rules to appropriately address risks;
- the prevention of improper use; and
- rules to ensure effective compliance.

The PPC is still conducting discussions regarding the issues highlighted in these documents. No clear timeline for the implementation of the results of such discussions has been made; specific proposed amendments to the APPI may be published as early as this spring, but it remains unclear whether all of the issues discussed in these documents will be reflected in such amendments.

Nevertheless, some of these discussions, if implemented, would undoubtedly have a significant impact on a wide range of businesses processing personal data in Japan. This chapter focuses on such key issues and summarises the status of the PPC's discussions thereon as of January 2026.

Note that one unique aspect of the APPI compared to other countries' data protection regulations is that it defines concepts such as “Personal Information”, “Personal Data” and “Personal Data the Business Holds”. Since most of the data processed by businesses falls under “Personal Data”, this chapter will use the term “Personal Data” without making strict distinctions between these terms.

Promotion of Proper Data Utilisation

Adjustment of consent requirements in the AI age

The current APPI requires businesses to obtain the consent of data subjects when acquiring sensitive personal data, such as race, medical history or crimi-

nal record (Article 20), or providing personal data to a third party (Article 27), among other activities. There have been complicated debates on how strictly these regulations should be applied in situations where training data sets containing personal data are used for AI development. This is said to have been causing confusion in practice.

The PPC is of the opinion that parameters making up a learned model of AI do not constitute personal data even if the model was trained with data sets containing personal data, as long as there is no correspondence between such parameters and a specific individual. However, this does not mean that AI developers may use personal data they received from a third party, such as user companies, without limitation for AI training purposes; instead, AI developers may only use such personal data without the data subjects' consent within the scope of work outsourced by the third party.

As a result, it is often discussed whether the usage of the subject training data sets falls "within the scope of work outsourced by the third party", which is hard to determine if the AI developer intends to provide the learned model to users other than the third party that provided the data sets. There is also a debate as to whether it would be illegal for an AI developer to create training data sets containing personal data without the data subjects' consent by collecting information that was publicly available on the internet but unintentionally containing sensitive personal data.

Under these circumstances, the PPC's Views on Institutional Issues and Policy on Institutional Amendments demonstrate that it is considering the introduction of a system that would allow for the legitimate provision of personal data to a third party and the acquisition of publicly available sensitive personal data without the data subjects' consent as long as it is ensured that such data would be used only for the creation of statistical information, including "AI development, etc., which can be categorised as statistical creation, etc." If such system is introduced, the practical confusion surrounding AI development would likely be settled to a certain extent.

Other directions regarding relaxation of consent requirements

In addition to the points mentioned above, the PPC's Views on Institutional Issues and Policy on Institutional Amendments also suggest that personal data processing that clearly does not contradict the data subject's will and therefore does not harm his/her rights and interests may be allowed without his/her consent. Such processing may include, for example, the provision of customer data from a hotel booking site to the hotel where the customer wishes to stay, or data sharing between banks for overseas remittances.

Consent may also no longer be required for the processing of personal data that is necessary for the protection of life, body or property, or for the improvement of public health or the promotion of the healthy development of children. Under the current APPI, such data processing is allowed without data subjects' consent only if it is difficult to obtain such consent. The PPC is considering easing the requirement by allowing such data processing even when it is not difficult to obtain the data subject's consent but there are reasonable grounds for not obtaining his/her consent – for example, when necessary and appropriate measures have been implemented to prevent privacy violations, such as anonymisation or concluding confidentiality agreements.

The PPC is also considering easing consent requirements when hospitals and other organisations providing medical care acquire sensitive personal data or share personal data with third parties.

Rules to Appropriately Address Risks

Establishment of new regulations on processing children's personal data

The current APPI does not have any special regulations regarding the processing of children's personal data that differ from those relating to adults, except that it stipulates that a legal representative, including a parent, may make a request for disclosure, etc., on a child's behalf (Article 37). On the other hand, the PPC makes it clear that, when processing the personal data of children under the age of 12, businesses should obtain the consent from the children's legal representatives rather than from the children themselves.

Under these circumstances, the PPC is considering taking further steps to establish new regulations on the processing of children's personal data, including:

- a regulation that would obligate businesses to obtain the consent of, or notify, the legal representatives of the data subjects with respect to the processing of personal data of children under the age of 16 that requires businesses to obtain the consent of, or notify, the data subjects; and
- a regulation that would allow children under the age of 16 or their legal representatives to, without cause, request businesses to cease to use, delete or cease to provide a third party with their personal data.

Establishment of new regulations on the processing of biological data

The current APPI does not have any special regulations regarding the processing of biological data that differ from those applicable to other personal data, unless it involves sensitive personal data.

However, biological data that can be easily obtained without the data subjects' knowledge and that can be used to track their behaviour over time due to its uniqueness and immutability, such as facial feature data, is prone to invade the privacy of data subjects, even if it is not sensitive personal data.

The PPC is therefore considering establishing new regulations on the processing of such biological data, including:

- a regulation that would obligate businesses that are processing such biological data to disclose certain items regarding the processing; and
- a regulation that would allow data subjects to request businesses to, without cause, cease to use, delete or cease to provide a third party with such biological data.

Adjustment of regulatory framework for businesses entrusted with personal data processing

The APPI currently requires businesses to obtain data subjects' consent when providing personal data to third parties, as discussed above, but there are some

exceptions. Specifically, data subjects' consent is not required when personal data is provided to a third party for the purpose of entrusting personal data processing (Article 27, Paragraph 5, Item 1). Instead, businesses must exercise necessary and appropriate supervision over such third-party processors (Article 25).

For instance, cloud service usage may be categorised as entrusted personal data processing. In such cases, cloud service users must supervise service providers, such as through requiring periodic reports on the status of personal data processing. However, such supervision may be impractical when small-scale businesses use large-scale cloud services.

Therefore, the PPC is now considering reviewing regulations for entities entrusted with personal data processing based on practical realities. For example, such entities may no longer be required to implement security measures for the entrusted personal data by themselves as long as they conclude agreements with the entrusting party regarding all aspects of the means of the processing and measures necessary for the entrusting party to monitor the status of the processing.

Adjustment of data breach notification requirements

The current APPI requires businesses that have experienced a specific type of personal data breach to report it to the PPC and notify the data subjects involved of such breach (Article 26).

"Personal data" in this context includes information such as a management ID assigned solely for internal system database integration, which by itself cannot identify a specific individual but can be easily collated with other information, such as the name and contact information of an individual, to thereby identify a specific individual. Businesses would therefore be required to comply with the reporting and notification obligations even if only such information had been breached, which as a result imposes an excessive burden on businesses.

Under these circumstances, the PPC is considering relaxing the obligation to notify data subjects of a data

breach in cases where there is little risk to individual rights and interests, including where only information such as the management ID, which has no meaning by itself for those who acquire it, has been breached. This is considered an issue that would have no small impact on practice.

Prevention of Improper Use

The current APPI only prohibits the inappropriate use or improper acquisition of personal data – ie, information that can identify a specific individual, either by itself or with other information that can easily be collated with it (Articles 19–20). In other words, the APPI does not currently regulate the inappropriate use or improper acquisition of information with which no specific individual can be identified.

However, the inappropriate use or improper acquisition of such information may also infringe individual rights and interests if the party using or acquiring it can contact the data subjects through such information. For example, a malicious party can send phishing emails to email addresses even if such email addresses do not constitute personal data – ie, no specific individual can be identified with the email addresses themselves or with other information that can easily be collated with them. In addition, anonymous health information that is not considered personal data can be used for advertising purposes beyond the purposes known to the data subjects.

Under these circumstances, the PPC is considering broadening the coverage of the prohibitions mentioned above by prohibiting the inappropriate use or improper acquisition of information with which no specific individual can be identified but through which the party using or acquiring it can contact the data subjects.

Rules to Ensure Effective Compliance

Introduction of an administrative monetary penalty system

If businesses processing personal data violate the current APPI, they may be subject to sanctions issued by the PPC, such as administrative guidance, advice, recommendations or other orders, publication of their non-compliance (Articles 147–148) or criminal penal-

ties, including fines of up to JPY100 million (Articles 178–179 and 182–185).

Based on the data published by the PPC, while several hundreds of notices of administrative guidance, advice and recommendations have been issued annually, including against major corporations, no orders have been issued to businesses engaged in normal business activities, and no criminal penalties have ever been imposed on companies. These facts have cast doubt on the deterrent effect of the current APPI and, given the fact that many other countries have already introduced financial penalty systems, discussions over the potential introduction of an administrative monetary penalty system in Japan have been increasing in recent years.

On the occasion of the current triennial review process, the PPC seems to be seriously considering the introduction of an administrative monetary penalty system for the APPI. However, it has been proposed that the scope of corporate acts that would be subject to monetary penalties should be limited to some extent, to avoid excessive regulation that might discourage lawful acts.

The proposal includes the introduction of a penalty that would be imposed on a business only when:

- it has derived financial benefits by violating any of the specific provisions of the APPI, including Articles 19 (prohibition of inappropriate use), 20 (proper acquisition) and 27 (restrictions on provision of personal data to third parties);
- it fails to exercise reasonable care to prevent such violation;
- individual rights and interests have been or are likely to be infringed by such violation; and
- the number of data subjects involved is not less than 1,000.

Ensuring the effectiveness of recommendations, orders, etc

In addition to the potential introduction of an administrative monetary penalty system, the PPC is considering the introduction of measures to ensure the effectiveness of existing penalties, such as recom-

mentations and orders issued by the PPC, as well as criminal penalties.

Specifically, the PPC is considering allowing the issuance of orders, which under the current APPI may be issued only when a business has violated the PPC's recommendations or individual rights and interests have been actually infringed, even when no recommendation has been issued, and individual rights and interests have not yet been infringed but are in imminent danger of being infringed.

The PPC is also considering allowing the issuance of recommendations or orders that recommend or require a business to take measures necessary to protect data subjects' rights and interests, including notifying the data subjects or publishing the fact that the business had violated the APPI.

On the other hand, while the Interim Report had suggested that the PPC was considering introducing injunctive relief and damage recovery systems through qualified consumer organisations, which might have been another means to ensure effective compliance of the APPI through new systems where consumer organisations may seek injunctive relief against businesses' acts that violate the APPI or seek collective recovery through the courts for moral damages caused due to businesses' negligent data breaches, the Policy on Institutional Amendments does not refer to such systems. It seems that the PPC does not consider the introduction of such systems to be among its highest priorities.

Conclusion

As mentioned earlier, the PPC is still discussing the issues described in the Interim Report, its Views on Institutional Issues, the Policy on Institutional Amendments and other documents, and it is uncertain when and how such discussions will conclude and be implemented in a concrete manner. Businesses processing personal data in Japan should continue to pay close attention to the developments of this ongoing triennial review process.

Law and Practice

Contributed by:

Alex Saleh, Asad Ahmad, Mohammed Nader Al Awadhi and Liana Rashid

GLA & Company



Contents

1. Legal and Regulatory Framework p.261

- 1.1 Overview of Data and Privacy-Related Laws p.261
- 1.2 Rights and Obligations p.262
- 1.3 Special Categories of Personal Data p.264
- 1.4 Processing of Personal Data for Research and Development Purposes p.264
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.265
- 1.6 Data Breach Requirement p.265
- 1.7 Regulators p.265
- 1.8 Enforcement Proceedings and Fines p.265
- 1.9 Enforcement Trends p.267

2. Privacy Litigation p.267

- 2.1 Privacy Litigation Overview p.267
- 2.2 Recent Case Law p.267
- 2.3 Collective Redress Mechanisms p.267

3. Requirements for the Protection and Processing of Non-Personal Data p.267

- 3.1 Objectives and Scope of Data Regulation p.267
- 3.2 Interaction of Data Regulation and Data Protection p.267
- 3.3 Rights and Obligations Under Applicable Data Regulation p.268
- 3.4 Regulators and Enforcement p.268

4. Sectoral Topics p.268

- 4.1 Use of Cookies p.268
- 4.2 Personalised Advertising and Other Online Marketing Practices p.268
- 4.3 Employment Privacy Law p.269
- 4.4 Data Protection in M&A p.269

5. International Considerations p.269

- 5.1 Restrictions on International Data Transfers p.269
- 5.2 Government Notifications and Approvals p.269
- 5.3 Data Localisation Requirements p.270
- 5.4 Blocking Statutes p.270
- 5.5 Recent Developments p.270

GLA & Company is the premier full-service regional law firm committed to delivering exceptional legal solutions across the Middle East and North Africa. With eight strategically located offices in seven key jurisdictions – UAE, KSA, Oman, Qatar, Kuwait, Bahrain and Egypt – the firm is positioned to serve its clients with unparalleled expertise and dedication. Founded

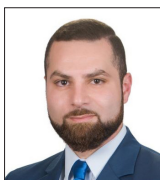
by a team of experienced legal professionals, GLA & Co has grown to encompass over 18 partners and more than 170 lawyers across the MENA region. Its diverse team is united by a shared commitment to excellence and a deep understanding of the unique legal landscapes of the jurisdictions it operates in.

Authors



Alex Saleh is the managing partner of GLA & Co and takes a leading regional role within the firm with respect to its Corporate & Commercial practice. With over 30 years of experience in both the GCC

markets as well as the US, he has accumulated sizeable expertise in the areas of banking and finance, mergers and acquisitions, capital market deals and infrastructure projects.



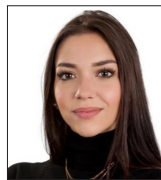
Asad Ahmad is the legal director and head of the Antitrust & Competition practice at GLA & Co, leading the firm's regional practice across Kuwait, KSA, Qatar, UAE, Egypt and COMESA. He advises clients on

merger control, competition compliance and regulatory matters, securing major clearances and handling high-profile investigations. Asad also leads GLA & Co's Data Privacy team, guiding multinational clients on regulatory compliance and data protection strategies. A dedicated mentor and thought leader, he contributes to legal publications, conducts webinars and actively engages with competition regulators, reinforcing GLA & Co's reputation as a leader in antitrust and competition law.



Mohammed Nader Al Awadhi is a corporate and commercial lawyer besides being a commercial and civil litigator representing multinational companies and joint ventures in connection with litigation and

possible litigation strategies. He also regularly leads and assists the corporate team in the Kuwait office of GLA & Co in their day-to-day matters, with a primary focus being legal issues arising out of corporate affairs in Kuwait. Mohammed prides himself in leading the firm on acquisitions in all sectors of the Kuwait and regional market.



Liana Rashid is an accomplished associate in GLA & Co's Kuwait office, bringing over three years of extensive legal experience across a diverse range of practice areas. A graduate of the University of Sheffield School of

Law, Liana has developed a strong foundation in litigation, mediation, employment law, data privacy, mergers and acquisitions, banking and competition law. Her bilingual proficiency in Arabic and English enables her to deliver high-quality legal advice to prominent clients in Kuwait and the GCC region, contributing to high-value transactions and managing cross-border matters with precision and expertise.

GLA & Company

Alex Saleh
Managing Partner

Tel: Kuwait: +(965) 669 55516
UAE: +(971) 54 997 4040
Email: alex.saleh@glaco.com
Web: glaco.com/attorneys/alex-saleh/



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Kuwait does not have a single, state-wide data protection statute; instead, privacy and data protection are governed by a mix of e-transaction rules, sectoral telecom rules, cloud guidance, cybercrime provisions and general media/content controls issued by respective data control authorities in Kuwait.

The principal instruments are the Electronic Transactions Law No 20 of 2014 (the “E-Transactions Law”) and its Executive Regulations (Decision No 48 of 2014) governing collection, use, disclosure, security and data subject rights for electronic records handled by public authorities and private entities, including consent and purpose specification for access/disclosure and duties to ensure accuracy and safeguards for personal data in electronic systems. Furthermore, the Cybercrime Law No 63 of 2015 criminalises unauthorised access, alteration, disclosure and destruction of data (including personal and governmental data), with escalating penalties depending on the nature of the systems and data affected.

Telecom-sector privacy is governed by the Kuwait Communication and IT Regulatory Authority (CITRA) Data Privacy Protection Regulation (DPPR), as amended by Decision No 26 of 2024, which now applies exclusively to CITRA-licensed telecom and internet providers (the “Licensees”) and imposes consent, transparency, security, transfer notice and breach notification duties on those Licensees. Additional instruments include CITRA’s Users’ Rights Pro-

tection and Regulation of Communications and IT Services (the “User Guidelines”) and CITRA’s Cloud Computing Regulatory Framework (v2.4) (the “Cloud Framework”), which prescribe collection/disclosure practices, security and transparency for Licensees and licensed cloud service providers (CSPs) operating data centres in Kuwait.

Additionally, the CITRA Law No 37 of 2014 (establishing CITRA), the Electronic Media Law No 8 of 2016 (regulating certain online publishers), and content blocking powers under press, cybercrime and telecom statutes interact with privacy by limiting certain data/content uses on public order and security grounds.

In terms of multi-level interaction, Kuwait’s framework is domestic and not tied to supranational regimes like the EU’s GDPR, and overlap occurs horizontally between general e-transaction obligations, cybercrime provisions and sector-specific telecom/cloud rules, with the E-Transactions Law acting as a general baseline and the DPPR/User Guidelines applying only to Licensees. That being said, certain rules have extraterritorial reach. For Licensees, the DPPR expressly captures data collection/processing performed inside or outside Kuwait, and requires transparency regarding transfers abroad. For other Kuwait entities, cross-border data handling defaults to the consent, purpose limitation and security duties under the E-Transactions Law.

Kuwait has not enacted a comprehensive AI law, and governance of AI-related personal data is therefore derived from the above instruments. There is no equivalent to the EU’s European Health Data Space

or Data Act; however, CSP and telecom rules impose transparency/security requirements, and the Electronic Media Law governs certain online publishing activities with privacy-intersecting content rules.

1.2 Rights and Obligations

The E-Transactions Law

Consent

Under Article 4 of the E-Transactions Law, individuals must consent prior to dealing by electronic means, though such consent may be inferred through affirmative conduct indicating approval.

Under Article 32, when collecting data (including personal data and data relating to individuals' professional affairs, social status, health status or financial status), government authorities, public authorities and institutions, companies, non-governmental entities and their employees ("Entities") are explicitly mandated to secure individuals' consent and to state the purpose behind collecting such data.

Under Articles 32 and 35, Entities must also ensure that consent is obtained when conducting any access, disclosure, sharing or processing of the collected data. These activities must be undertaken by lawful means and be limited to the stated purpose provided to data subjects. This is a requirement that pertains to personal data or information that is stored in electronic records or processing systems and relates to the professional affairs, social status, health status or financial status of individuals who are registered with the Entities.

Data protection

Under Article 35, Entities are required to regularly verify and update the accuracy of personal data or information stored on their electronic records or processing systems. They must also implement appropriate measures to safeguard the personal data and information collected or stored on their electronic records or processing systems.

Under Article 2 of the Executive Regulations, the storage and maintenance of electronic records, inclusive of personal data, must preserve their original form, encompassing all associated original data, without compromising the quality or standard of the records.

In addition, the storage of electronic records, inclusive of personal data, should align with the policies and agreements established between the parties involved in electronic transactions, specifying the duration for retaining and maintaining such records.

Data subject rights

Article 33 of the E-Transactions Law grants specific rights to data subjects concerning their personal data stored in electronic records and processing systems maintained by Entities. Any person with their personal data stored by an Entity has the right to request access to, as well as a record of, such data.

Additionally, under Article 36, the data subject has the right to modify or delete their personal data held by any Entity, and may also update personal information in the event of changes. Requests for the access, modification or deletion of personal data can only be initiated by the individual to whom the data pertains or by their legal representative (Articles 25–26 (1) of the Executive Regulations).

Under Article 26 (2) of the Executive Regulations, deleting stored personal data or information is only permissible when correction is deemed necessary; in such cases, the previously stored information must be maintained without any use or handling.

The User Guidelines

Collection of data

Under Article 2 of the User Guidelines, a Licensee must prepare relevant rules and mechanisms for the sale of its service, either through means of electronic transaction or through telephone communication. CITRA must approve the rules and mechanisms (or any amendments to existing contracts of sale) in advance, which includes the relevant data collection and storage rules and mechanisms. Pursuant to Article 3.16, in the case of any amendment to an existing contract of sale, the following must occur before execution can take place:

- the service user must be notified of the amendment 60 days before the amendment enters into force; and
- the service user's written approval or e-signature (using the "Hawyti" application) must be obtained.

Under Article 3.3, the Licensee must verify the validity of the personal information provided by the users of said services; such proof (in the form of a civil ID, passport or driving licence) must be certified by competent governmental bodies.

Under Article 3.4, before executing the service contract, the mechanism(s) for cancelling the service and any variation(s) to the contractual terms of service must be clearly stipulated.

Under Article 3.6, the Licensee must open an electronic file in which all the information, documents and complaints pertaining to each user are safely stored.

Duties of the Licensee upon a user's request for cancellation of service

Under Article 4, the Licensee must facilitate the mechanisms or procedures for cancellation of service. The Licensee may not bind the subscriber with a minimum limit of the service contract term, unless this is approved by the authority. Upon the subscriber's request to cancel the service, the Licensee must verify the identity of the subscriber applying for cancellation.

Dealing with data

Under Article 6, Licensees must adhere to the following requirements:

- Making no collection, use or disclosure of any personal information relating to the user without their explicit approval.
- Not requiring information that is irrelevant in the context of providing services.
- Obtaining the approval of the user before disclosing their information to other parties.
- Taking all security measures with regard to:
 - (a) protection of the user's information; and
 - (b) protection against the loss, damage or disclosure of such information (or its replacement with any untrue data).

The DPPR *Consent*

Under Articles 2 and 4 of the DPPR, Licensees must secure user consent prior to collecting and processing their personal data, and must specify the purpose for data collection and processing both before and

during the provision of services, as well as after the termination of services.

Data protection

In accordance with Article 5 (1-3), Licensees are required to implement robust measures for safeguarding data from unauthorised access, loss, destruction or damage, with protective measures to include encryption, confidentiality practices and disaster recovery protocols.

Under Article 6, Licensees must inform both the data subject and CITRA in the event of a personal data breach.

Data subject rights

Under Article 4 (3), Licensees must disclose their identity, location and contact information to their users, ensuring that users can readily recognise and reach out to them when required.

Under Article 4 (10), users must be given the right to withdraw consent or to entirely delete their personal information from a Licensee's records.

Under Article 4 (11), Licensees are obliged to notify data subjects if their personal data is to be transferred outside Kuwait.

Under Article 4 (12), Licensees must afford their users the right to access or modify stored personal data that is in their possession and is stored with them.

CITRA Cloud Service Providers: Regulations and Commitments

Types of information collected by CSPs

Pursuant to the regulations concerning Platform as a Service (PaaS) and Software as a Service (SaaS) providers in Article 2 of the Cloud Framework, the types of information that a CSP may obtain from a user include (but are not limited to):

- name and email address;
- address;
- payment information;
- internet protocol address ("IP address"); and
- device and browser information.

Obligations in dealing with information

In accordance with the regulations concerning PaaS and SaaS providers in Article 2, the CSP must describe to the user all information that needs to be collected and inform them as to what information will be collected automatically (as well as where to access and amend such information). Following data collection, the CSP must explain to the user where and how such information may be used.

The CSP may not use this information to determine the identity of the user. The CSP must also inform the user of any third-party providers that operate certain services on its behalf – and of its privacy policies – for the purpose of maintaining transparency. The CSP commits to not share, dispose of or sell the user's information with third parties; however, for purposes of improving the service and customer experience, it may be granted access to the user's name, address, phone number and email. In any case, the user must be informed of such.

The user must be notified immediately of any relocation of data to new owners as a result of M&A, liquidation or dissolution.

The CSP must be efficient, competent and equipped to detect any fraud, security threats or technical problems.

The user has the right to request the amendment or deletion of their personal data available to the CSP or to third parties. The CSP must also provide clear mechanisms to users for communication regarding the privacy policy.

SaaS providers must specify in their privacy policy the targeted age group for the collection of data. If the targeted age group is minors, the consent of their guardians must be obtained. The service must abide by any relevant child protection laws of the state.

A practical compliance checklist would commonly include:

- map electronic records and personal data flows (including cloud/telecom dependencies);
- implement consent and purpose disclosures;

- deploy access, correction and deletion mechanisms;
- adopt security and retention controls consistent with the E-Transactions Law and DPPR rules;
- enable breach identification and notification procedures (applicable to Licensees with respect to notification of CITRA and users);
- ensure transfer transparency and approvals where required; and
- maintain clear user-facing privacy policies and change-control processes.

1.3 Special Categories of Personal Data

Kuwait's legal instruments do not provide a GDPR-like taxonomy of "special categories", but the E-Transactions Law does make reference to personal data as data stored in electronic systems relating to an individual's professional, social, health or financial status, with criminal sanctions for unlawful access/disclosure/use or processing beyond stated purposes.

Processing minors' data requires guardian consent when SaaS targets minors (under the User Guidelines). Providers must state any age targeting in their privacy policy and comply with child protection requirements.

There is no standalone regime for criminal conviction data beyond the general prohibitions and criminal penalties for unlawful access, alteration or disclosure under the Cybercrime Law and the E-Transactions Law.

1.4 Processing of Personal Data for Research and Development Purposes

Kuwait has not adopted a dedicated secondary-use regime akin to the EU's European Health Data Space. Secondary use for product development or research typically relies on processing consent requirements pursuant to the E-Transactions Law and the DPPR principles on data collection and processing purpose specification, lawful means and security outlined in **1.2 Rights and Obligations**.

For medical data, written patient consent is generally required for disclosure, and healthcare providers must maintain secure patient records under the Medical Profession Law No 70 of 2020. In practice, life

sciences and healthtech companies implement de-identification methods and limit re-identification risks.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

There is no dedicated AI statute in Kuwait. Personal data used in AI systems must comply with the E-Transactions Law's consent, purpose, accuracy and security principles, and with DPPR/User Guidelines where the entity is a Licensee handling subscriber data.

1.6 Data Breach Requirement

For Licensees, the DPPR requires notifying both CITRA and affected data subjects in the event of a personal data breach within a time period not exceeding 24 hours from the time of breach, supported by appropriate technical measures and incident response capabilities. The notification must set out the nature of the breach, including the scope of the personal data leakage, the categories of affected individuals, and the security levels impacted, together with the identity of the Licensee's Data Protection Officer and the means of communicating with that officer. It must further address the potential consequences of the breach and outline the measures already taken or proposed by the Licensee to mitigate and address the breach. Notification to the affected data subjects is not required where the Licensee has implemented appropriate technical and organisational protection measures and such measures have been applied to the personal data subject to the breach.

For other entities, breach handling is guided by the E-Transactions Law's security and lawful processing duties, and the Cybercrime Law applies to unlawful access, alteration or disclosure, and the competent authorities may initiate investigations in the event that any complaints or referrals indicate offences.

1.7 Regulators

Kuwait does not currently have a single regulatory authority with overarching jurisdiction over data protection matters.

While CITRA was initially regarded as the principal data protection regulator (given that the DPPR originally imposed obligations on a broad range of entities), subsequent amendments have limited its direct regu-

latory scope primarily to Licensees. Notwithstanding this narrowing, CITRA continues to play a significant role by overseeing various data protection-related matters, issuing regulations and providing guidance, particularly within the telecommunications sector applicable to Licensees.

In parallel, the Central Agency for Information Technology serves as another key authority in the area of personal data protection, being responsible for the issuance of the E-Transactions Law and its Executive Regulations.

In addition, the National Centre for Cybersecurity, established pursuant to Decree No 37 of 2022, is a recently formed authority with a central regulatory role in cybersecurity matters, particularly in relation to governmental entities.

Regulatory investigations are generally initiated following complaints or through supervisory oversight. In this context, CITRA has the authority to conduct inspections, assess service quality, review relevant records, require corrective measures and, where criminal conduct is suspected, refer matters involving Licensees to the competent authorities.

1.8 Enforcement Proceedings and Fines The CITRA Law

The CITRA Law empowers CITRA to collect information relevant to the telecommunications and IT sectors, and to issue any reports, bulletins and guidelines to users. CITRA, pursuant to the CITRA Law, also prepares the necessary media programmes to increase public awareness of the importance attached to these sectors and the extent of their influence on social and economic development in the State of Kuwait.

Pursuant to Article 15 of the CITRA Law, all Licensees must adjust their internal policies and rules to any extent necessary to achieve compliance with the provisions of the CITRA Law.

Pursuant to Article 49 of the CITRA Law, if CITRA receives any complaint about a Licensee's default in the performance of its obligations, a dispute between a Licensee and beneficiary users in relation to the quality and standard of the service being provided or

any violations of the licence conditions, CITRA may investigate the complaint and make a decision to either not pursue any action or notify the Licensee to remove the violation within 90 days.

Under Article 52 of the CITRA Law, CITRA must decide with the Licensee on the procedures for any investigations into complaints.

Under Article 54 of the CITRA Law, CITRA must ensure that the Licensee complies with all the provisions of the CITRA Law, and may take any actions it deems necessary in order to do so, such as:

- conducting physical examination(s) of the network and telecommunications devices;
- examining the Licensee's technical records to ensure invoices and records are accurate;
- assuring the quality of the services and adequacy of the complaint procedures provided to clients; and
- reviewing the maintenance and failure records of the Licensee to ensure the management service is efficient.

Lastly, under the CITRA Law, CITRA must also ensure compliance with any international, regional and bilateral agreements to which Kuwait is a party.

Executive Regulations of the CITRA Law Under Decision No 933 of 2015 (the "CITRA Regulations")

Under the CITRA Regulations, CITRA may refer a matter to other competent authorities if – following investigation(s) – there are reasons to suspect a criminal offence. Employees of CITRA are empowered to monitor the implementation of CITRA's laws and regulations. To this end, they have the right to enter places in order to inspect and control any unlicensed communications devices where the following are known or suspected to be present:

- devices or networks;
- communications facilities; and/or
- all or part of the infrastructure used in the communications service.

In the process of doing so, the employees are empowered to:

- request and examine the Licensee's licences, records and documents;
- examine and view any communications equipment related to the provision of the service; and
- view any form of information or documents related to the provision of the services.

The E-Transactions Law

Under Article 37 of the E-Transactions Law, individuals who unlawfully access, disclose or publish any personal data registered in records or electronic processing systems of the relevant entities, related to the professional affairs, social status, health or financial status of individuals, whether registered with the entities or their employees, without the consent of the data subject or their legal representative, may face imprisonment for up to three years and a fine ranging from KWD5,000 to KWD20,000. Confiscation of the tools, programs or devices used in the commission of the offence may also be ordered.

Under Article 37, entities that collect, register or process any of the personal data stored with them on their electronic records or processing systems, using unlawful methods or without the consent of the person concerned or their legal representative, or that use the stored personal data for reasons other than those for which it was collected, may face imprisonment for up to three years and a fine ranging from KWD5,000 to KWD20,000. Confiscation of the tools, programs or devices used in the commission of the offence may also be ordered.

The Cybercrime Law

The Cybercrime Law addresses various forms of illegal access to electronic systems and data. It applies to individuals who unlawfully gain access to a computer, system, data processing system, automated system or information network. The penalty for such actions is imprisonment for up to six months or a fine ranging from KWD500 to KWD2,000, or both. If the illegal access leads to the deletion, alteration, damage or unauthorised disclosure of data, the punishment increases to up to three years in prison and a fine between KWD3,000 and KWD10,000, especially if the data is personal (Article 2).

The law also applies to those who illegally access government systems to obtain confidential information, whether directly or via the internet or other technological means. The penalty is imprisonment for up to three years or a fine ranging from KWD3,000 to KWD10,000, or both. If the access results in the alteration, deletion or disclosure of the data, the punishment escalates to imprisonment for up to ten years or a fine of between KWD5,000 and KWD20,000, or both. This provision also covers data related to clients' bank accounts (Article 3).

Additionally, the law applies to individuals who deliberately modify or destroy electronic medical documents related to medical tests, diagnoses, care or treatment, using the internet or other information technology. Those found guilty of such actions face imprisonment for up to three years or a fine of between KWD3,000 and KWD10,000, or both (Article 3).

1.9 Enforcement Trends

Two trends stand out in the last 24 months: the narrowing of the DPPR to apply only to telecom Licensees (under Decision No 26 of 2024) and the repeal of the Data Classification Policy (see **5.5 Recent Developments**).

Public visibility into administrative proceedings and fines remains limited, as regulators do not generally publish case-level outcomes. Accordingly, organisations (whether characterised as a Licensee or any other entity) should implement preventative controls and provide for clear consent and purpose mechanisms for collected personal data whether provided for under the E-Transactions Law or the DPPR.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Privacy litigation in Kuwait remains limited, with no publicly visible court disputes focused specifically on personal data protection.

Where disputes arise, they more commonly track cybercrime and unlawful access or disclosure obligations and violations handled through criminal channels under the Cybercrime Law and the E-Transactions

Law's penal provisions, rather than standalone civil damages claims for privacy harms. Non-material damages are not addressed as a distinct head of claim in the above-outlined laws and regulations.

2.2 Recent Case Law

Please see **2.1 Privacy Litigation Overview**.

2.3 Collective Redress Mechanisms

There is no specific collective redress regime for privacy claims reported in the above-cited legislation, and no recent developments implementing representative action mechanisms akin to the EU framework.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Kuwait does not have a cross-sector "data act", and regulation relevant to non-personal data largely consists in certain regulations applicable to Licensees. For example, the Cloud Framework applies to CSPs licensed in Kuwait operating data centres domestically and imposes transparency and security obligations on providers and practical commitments that affect subscribers' data handling across personal and non-personal data.

The DPPR now applies only to Licensees, while the E-Transactions Law applies broadly to entities handling electronic records, providing protections and obligations regarding collection, disclosure, security and record maintenance.

The Electronic Media Law governs certain online publishing services and content, whereby online Kuwait platforms must comply with rules tied to public order and morals catering to Kuwait's culture and the Islamic faith.

3.2 Interaction of Data Regulation and Data Protection

The Electronic Media Law applies to and regulates various online platforms, including:

- electronic publishers;
- electronic journalism;

- news agencies;
- news services;
- websites offering electronic commercial advertisements; and
- the digital presence of print newspapers and satellite channels.

However, the Electronic Media Law does not apply to personal domains, websites, outlets or electronic accounts that are not operated by individuals with specialised professional expertise. Notably, the Electronic Media Law specifies that the name of the website or media outlet must not violate public order or morals or be identical to an existing site. Thus, media regulation under Kuwaiti law seems to be restricted to media channels that are not privately owned. On the other hand, the data protection requirements under the E-Transactions Law or the DPPR would apply to both private companies and entities offering services to the public.

3.3 Rights and Obligations Under Applicable Data Regulation

Under the E-Transactions Law, individuals have rights to access, correction and deletion of personal data in electronic records, while entities must ensure accuracy, purpose limitation and security, with retention aligned to policies and agreements.

The DPPR and User Guidelines impose Licensee-specific obligations on consent, transparency, breach notifications to CITRA/users, and transfer notifications for data leaving Kuwait.

The Cloud Framework requires privacy policies to cover categories of data collected, use and disclosure practices (including third-party processors), cookie usage, marketing unsubscribe mechanisms and user correction/deletion pathways, with alerts on data relocation due to M&A or ownership changes. There is no statutory data portability right, and organisations should instead enable reasonable access on a contractual and transparency basis.

For action items, please also see **1.2 Rights and Obligations**.

3.4 Regulators and Enforcement

Please see **1.7 Regulators**.

4. Sectoral Topics

4.1 Use of Cookies

Pursuant to the Cloud Framework, the privacy policy of a CSP must contain a clause labelled “Cookies”, which determines the mechanisms of usage when it comes to:

- log-in authentication;
- security inferences;
- advertisements; and
- personal identification.

The CSP may not use this data to determine the identity of the user and must always disclose the types of cookies used by it or by external parties on any platform on which the service operates.

4.2 Personalised Advertising and Other Online Marketing Practices Spam Messaging

In accordance with Article 12 of the CITRA Regulations, the Licensee must have a database of users who have requested that they do not receive spam messages. Licensees sending messages for commercial purposes must only do so between the hours of 7am and 10pm Kuwait time.

Marketing Practice

Pursuant to Article 14 of the User Guidelines, the marketing practices of Licensees must not exploit any consumer or group of consumers on account of their weaknesses, disabilities, ages or lack of knowledge. They must also not use any means of fraud or deception in the advertising of their products and services.

When it comes to sending a marketing communication/call, the Licensees must have duly verified the identity of the recipient user. At the beginning of the communication/call, the Licensee must:

- disclose the sender’s name;
- disclose the cause for such communication/call; and

- give the recipient user the option to continue with the communication/call or not.

Regulations and Commitments of CSPs

The CSP's privacy policy must inform users of the procedures to follow should they wish to cancel marketing communication subscriptions.

4.3 Employment Privacy Law

Law No 9 of 2001 Regarding Misuse of Telecommunications and Wiretap Sets governs privacy in an employment context, but there is no specific rule applicable to employee monitoring.

Telephone conversations may be recorded by employers to deal with any grievances from customers or clients, in order to ensure that the calls are dealt with professionally or for the purposes of training only. In some situations, such recordings may be carried out and reproduced for legal purposes upon an order of the competent court in a situation occurring between third parties and company employees.

No applicable laws are in place for monitoring employees' emails in Kuwait. Private life cannot be violated, so the monitoring and recording of such information is considered to be an infringement of rights and a violation of confidentiality, which is guaranteed to individuals under the Kuwaiti Constitution. The courts of Kuwait aim to protect citizens and expatriates from all such violations. The employer can draw up a set of rules and regulations that may govern such monitoring for the purpose of safeguarding their interests. However, they should restrict it to the official work areas and not infringe on privacy rights, including the protection of personal emails. Such rules and regulations will need to be drawn up and made available to employees in a handbook that is provided to newly joined employees for them to understand and abide by.

4.4 Data Protection in M&A

The E-Transactions Law

Under Articles 32 and 35 of the E-Transactions Law, Entities are expressly required to:

- obtain individuals' consent before accessing, disclosing or sharing personal data; and

- specify the purpose for collecting and processing such personal data, including processing activities for data transfers.

These activities must be conducted using lawful means and limited to the stated purpose. This applies to personal data or information in electronic records or processing systems concerning the professional, social, health or financial status of individuals registered with these Entities. Consent may be obtained or inferred from affirmative actions indicating approval, as outlined in Article 4 of the E-Transactions Law.

DPPR and the User Guidelines

Licensees have notification obligations, including informing data subjects about personal data transfers outside Kuwait, pursuant to Article 4 of the DPPR. In addition, Licensees are required to establish and uphold a written privacy policy that elaborates extensively on their procedures concerning the collection and processing of personal data, including transfers as part of the processing activities. This policy should be publicly accessible on their websites and provided to users and data subjects when entering into service contracts.

5. International Considerations

5.1 Restrictions on International Data Transfers

For entities operating under the E-Transactions Law, cross-border disclosures must align with consent, purpose limitation and security duties for electronic records.

For Licensees, the DPPR requires informing users of transfers of data outside Kuwait and their legal representative in the recipient country.

Please also see 4.4 Data Protection in M&A.

5.2 Government Notifications and Approvals

Private entities covered by the E-Transactions Law typically do not need regulatory approval for international data transfers, unless the data involves state or government-related information in Kuwait.

Licensees may require approval from CITRA to transfer user data internationally, as indicated through consultations with CITRA. However, there is a lack of specific regulations detailing the mechanisms or conditions for such data transfers.

5.3 Data Localisation Requirements

Kuwaiti law does not generally address data localisation requirements, especially after the repeal of the Data Classification Policy (see **5.5 Recent Developments**). However, certain sector-specific examples, such as a healthcare facility, must maintain a register and database to document patient information in either written or electronic form. The facility's management is responsible for ensuring the safety of these records, and, if the facility ceases operations or changes activities, it must provide its patients with files or copies of their medical information upon request (Article 60 of Law No 70 of 2020 on the Medical Profession). While the law does not provide specific mechanisms for data transfers, it is understood from the E-Transactions Law that patient consent is required.

Another example of data localisation is found in Article 80 of Law No 6 of 2010 on Labour in the Private Sector, which mandates that employers must maintain a dedicated file for each employee, containing essential documents such as the work permit, employment contract, civil ID, and records of leave, overtime, work injuries and penalties. Similar to healthcare facilities, this law does not address mechanisms for data transfers.

5.4 Blocking Statutes

Kuwait has several laws and regulations relating to blocking or censoring web content, some of which concern privacy and data protection. Key examples include the following:

- The Press and Publications Law No 3 of 2006 regulates the publication of printed and electronic media in Kuwait. It includes provisions relating to blocking content that violates public order, morals or national security. This law gives the government the power to block websites or other media that violate these provisions.

- The Cybercrime Law criminalises a wide range of online activities, including hacking and online fraud. This law gives the government the power to block websites or other online content that violates its provisions.
- The CITRA Law regulates the telecommunications sector in Kuwait and includes provisions relating to blocking or intercepting communications that violate public order, morals or national security. This law gives the government the power to block websites or other online content that violates these provisions.

Among other prohibited content, CITRA receives requests to block web content in Kuwait that violates the public interest (including public morals, Islamic faith teachings and public order). If CITRA receives a request to block or unblock web content, it will take the necessary actions to block prohibited web content or to unblock web content in the case of an error in classifying the content as prohibited.

5.5 Recent Developments

Following the repeal of the Data Classification Policy in February 2024, which previously classified sensitive data into different tiers, the regulatory framework for data storage and transfers has become less clear. Under the former policy, Tier 3 data (private sensitive data) included information such as business plans, internal reports, litigation files, medical records and criminal fingerprints, which, if disclosed without authorisation, could damage individual privacy. Tier 4 data, considered highly sensitive, included information of a national or governmental nature, and unauthorised disclosure of such data could cause significant harm to privacy.

The Data Classification Policy required that Tier 4 data be stored within Kuwait, while Tier 3 data could be stored in hybrid clouds, both inside and outside Kuwait. Due to the repeal of the Data Classification Policy, the legislative framework surrounding the storage and transfer of sensitive data is now governed primarily by the consent provisions in the E-Transactions Law.

MACAU SAR, CHINA

Law and Practice

Contributed by:

Pedro Cortés and Luís Rôlo

Lektou – Advogados e Notários

Contents

- 1. Legal and Regulatory Framework p.273**
 - 1.1 Overview of Data and Privacy-Related Laws p.273
 - 1.2 Rights and Obligations p.273
 - 1.3 Special Categories of Personal Data p.273
 - 1.4 Processing of Personal Data for Research and Development Purposes p.274
 - 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.274
 - 1.6 Data Breach Requirement p.274
 - 1.7 Regulators p.274
 - 1.8 Enforcement Proceedings and Fines p.274
 - 1.9 Enforcement Trends p.277
- 2. Privacy Litigation p.277**
 - 2.1 Privacy Litigation Overview p.277
 - 2.2 Recent Case Law p.277
 - 2.3 Collective Redress Mechanisms p.277
- 3. Requirements for the Protection and Processing of Non-Personal Data p.277**
 - 3.1 Objectives and Scope of Data Regulation p.277
 - 3.2 Interaction of Data Regulation and Data Protection p.278
 - 3.3 Rights and Obligations Under Applicable Data Regulation p.278
 - 3.4 Regulators and Enforcement p.278
- 4. Sectoral Topics p.278**
 - 4.1 Use of Cookies p.278
 - 4.2 Personalised Advertising and Other Online Marketing Practices p.278
 - 4.3 Employment Privacy Law p.278
 - 4.4 Data Protection in M&A p.279
- 5. International Considerations p.279**
 - 5.1 Restrictions on International Data Transfers p.279
 - 5.2 Government Notifications and Approvals p.279
 - 5.3 Data Localisation Requirements p.280
 - 5.4 Blocking Statutes p.280
 - 5.5 Recent Developments p.280

Lektou – Advogados e Notários is a Macau SAR-based law firm with more than 40 years' experience of legal practice. Services regularly provided by the firm include advising on Macau law, helping international companies start their businesses in Macau, and assisting in the reorganisation of economic groups with connections to Macau. In 2016, Lektou partnered with Zhong Yin Law Firm (People's Republic of China – PRC) and CCW Law Firm (Hong Kong) to open a new office in Hengqin Island, Zhuhai, PRC

– ZLC Law Firm. This was the first law office to unite firms from the two Special Administrative Regions and Mainland China. Since then, it has extended and opened an office in Shenzhen. In 2017, Lektou extended its operations to Lisbon, Portugal, through Lektou – Cortés, Sociedade de Advogados, SP, RL, as part of its internationalisation strategy to position itself as a legal player in the platform between the PRC and Portuguese-speaking countries

Authors



Pedro Cortés is managing partner of Lektou, where he initiated his career as a lawyer in 2003, with experience in gaming, corporate and M&A, capital markets, and banking and finance. He is admitted to practise

law in Macau, Portugal, Brazil (São Paulo), China (as a cross-border Macau lawyer) and in East Timor. He is a member of the International Association of Gaming Advisors (IAGA), the Hong Kong Institute of Directors (HKIoD), International Masters of Gaming Law (IMGL), the International Bar Association (IBA), the Chartered Institute of Arbitrators (CIArb) and the Hong Kong Institute of Arbitrators (HKIA). Pedro is a guest lecturer at the Portuguese Catholic University – Lisbon School of Law, and of the Autónoma Academy in Lisbon.



Luís Rôlo is currently a trainee lawyer with Lektou, having joined the firm in 2020. He graduated from the University of Macau in 2008 and is registered with the Macau Lawyers Association. His professional

background includes being a senior officer at the Macau Pension Fund (1988–99), a senior officer at the Financial Services Bureau (1999–2010), a jurist at the Cabinet of the Commissioner Against Corruption (2010–14) and a jurist at the Office for Personal Data Protection (2014–18).

Lektou – Advogados e Notários

Avenida da Amizade, 555
Landmark Office Tower
23rd Floor
Macau SAR

Tel: +853 2856 2322
Fax: +853 2858 0991
Email: mail@lektou.com
Web: www.lektou.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Macau Special Administrative Region of the People's Republic of China (Macau SAR or MSAR) has its political and legal framework in the Basic Law, adopted by the National People's Congress in 1993, under the provision of Article 31 of the Constitution.

Data privacy and personal data protection are two rights enshrined by the Basic Law, which covers these two separate but related rights in a systematic and extensive manner.

The most relevant pieces of legislation addressing data protection and data privacy issues in Macau are:

- the Macau Basic Law;
- the Section of the Macau Civil Code on privacy and personal rights, enacted in 1999; and
- Law No 8/2005, the Macau Personal Data Protection Act (PDPA).

The latter is an act inspired by the former European legislation on data protection, namely the European Union Data Protection Directive of 1995, and sets the legal framework for the protection of personal data in Macau SAR.

Other legislation affecting this area that should be noted includes:

- Administrative Regulation No 42/2023, effective from 1 February, 2024, which created the Personal Data Protection Bureau (PDPB);
- a set of generic authorisations, legal opinions and case analyses that have been published by the PDPB on its official website; and
- Law No 2/2012, on the legal regime for video surveillance in public spaces and, pursuant to this act, the Dispatches of the Secretary for Security, authorising the specific setting up of video surveillance cameras in public spaces.

The government consistently includes a statement of priority in the annual policy address regarding the implementation of e-government, smart city and other

areas involving sensitive digital technologies and artificial intelligence.

Notwithstanding this, since its enactment in 2005, the PDPA has not been amended.

The international trend for amendments and updates of legal frameworks on data protection matters, as well as the continued domestic and international interest in the area, has not been reflected in amendments to the PDPA.

The legislation has no extraterritorial reach.

Separate legislation (Law 13/2019) provides for cybersecurity, covering networks and IT systems, with specific focus on operators of critical infrastructures.

1.2 Rights and Obligations

The general principle of transparency of processing is supplemented by specific principles, as provided by Articles 2, 5 and 6 of the PDPA:

- lawfulness and good faith;
- purpose limitation;
- adequacy and proportionality;
- accuracy;
- time limitation; and
- legitimacy by consent of the data subject or by prevailing legitimate interest of the controller.

Organisations carrying out processing of personal data should comply with the duty to notify the Regulator of the processing, within eight days the initiation of processing. The PDPB provides a structured and itemised form for the notification.

Besides the general duty of notification, organisations need to apply, unless otherwise provided by law, for authorisation for conducting some types of processing, namely when involving sensitive personal data, data relating to credit and solvency, combination of personal data and further processing of data for purposes not giving rise to their collection.

1.3 Special Categories of Personal Data

Sensitive personal data (Article 7 of the PDPA) is stated to be “data revealing philosophical or political

beliefs, political association or trade-union membership, religion, privacy and racial or ethnic origin, and data concerning health or sex life, including genetic data”. As a general rule, the processing of sensitive personal data is prohibited.

Processing of sensitive personal data, when allowed, must guarantee non-discrimination and be carried out with special security measures.

Processing of sensitive personal data may be allowed by a legal provision, under “important public interest grounds” and by “explicit consent” of the data subject.

Data relating to minors is not specifically addressed by legislation.

Data on suspicion of illegal activities, criminal and administrative offences (Article 8 of the PDPA) is restricted to “when such processing is necessary for pursuing the legitimate purposes of the controller, provided the fundamental rights and freedoms of the data subject are not overriding”. Central registers may only be created or kept by public authorities and data “for the purposes of police investigations shall be restricted to the processing necessary to prevent a specific danger or to prosecute a particular offence”.

1.4 Processing of Personal Data for Research and Development Purposes

Data relating to health and sex life, including genetic data, may be processed for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided that data is processed by a health professional bound by professional secrecy.

If data is adequately anonymised, it becomes no longer related to an “identified or identifiable natural person”, and is no longer deemed “personal data”.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Macau does not have specific privacy requirements for the use of personal data in the context of AI.

1.6 Data Breach Requirement

Under the cybersecurity law, private operators of critical infrastructures must inform the competent authority (the “Cybersecurity Committee”) of any “cybersecurity incident”. The PDPB is a member of the Cybersecurity Committee.

Notwithstanding, the PDPA does not require specific actions in the event of data breaches.

1.7 Regulators

The PDPB is, under Administrative Regulation 42/2023, the government entity responsible and accountable for monitoring and enforcing compliance with PDPA provisions, and for establishing an adequate confidentiality system and monitoring its enforcement.

The PDPB is granted powers covering a broad area of activities both in the private and in the public sectors and possesses a full legal basis and a permanent status.

Being a Bureau within the Public Administration of the MSAR, but reporting directly to the Chief Executive, it remains to be clarified whether this status equates with a status of permanent independence.

The PDPB is a member of the Asia Pacific Privacy Authorities (APPA).

Following its admission as an observer at the 30th Conference of the Global Privacy Assembly (GPA) in 2008, the current status of the PDPB is still observer, renewed at the 47th Conference in September 2025.

Guidance and recommendations issued by the PDPB are not binding but are generally adopted.

1.8 Enforcement Proceedings and Fines

There are two different types of administrative process: notification and authorisation.

Notification

Under the PDPA, the data controller, or their representative, if any, must notify the public authority in writing within eight days after the start of carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single pur-

pose or several related purposes. The public authority may authorise the simplification of, or exemption from, notification for specific categories of processing which, taking account of the data to be processed, are unlikely to adversely affect the rights and freedoms of the data subjects. In allowing this simplification or exemption, the authority will also consider the speed, economy and efficiency of the relevant processing.

The authorisation of simplification shall be published in the Official Gazette of the Macau SAR and must specify: the purposes of the processing; the data or category of data to be processed; the category or categories of data subjects; the recipients, or categories of recipients, to whom the data may be disclosed; and the length of time the data is to be stored.

There are exemptions from notification, such as those for processing whose sole purpose is the keeping of a register which, according to laws or administrative regulations, is intended to provide information to the public and which is open to consultation by the public in general or by any person demonstrating a legitimate interest.

The texts of these generic authorisations are available at the PDPB's official website.

Authorisation

Prior authorisation by the PDPB is required for some types of processing. These include the processing of sensitive data (where it is not carried out pursuant to a legal provision or it is carried out without the explicit consent of the data subject), data related to the credit and solvency of the data subject, and the combination of data and further processing of data for purposes other than those originally stated by the controller.

For this purpose, sensitive data means personal data revealing philosophical or political beliefs, political association or trade union membership, religion, private life, and racial or ethnic origin, and data concerning health or sex life, including genetic data. The authorisations for these types of processing shall be granted only if the controller provides guarantees of non-discrimination and sufficient security measures (indicated in the PDPA).

Applications submitted to the PDPB for opinions, authorisations and notifications shall include the following information:

- the name and address of the controller and of their representative, if any;
- the purposes of the processing;
- a description of the category or categories of data subjects and of the data or categories of personal data relating to them;
- the recipients or categories of recipients to whom the data might be disclosed and in what circumstances;
- the body entrusted with processing the information, if it is not the controller themselves;
- any combinations of personal data processing;
- the length of time for which personal data will be kept;
- the form and circumstances in which the data subjects may be informed of, or may correct, the personal data relating to them;
- proposed transfers of data to third countries or territories; and
- a general description enabling a preliminary assessment to be made of the adequacy of the measures taken to ensure security.

Without prejudice to the right to submit a complaint to the public authority, according to the law any person may have recourse to administrative and legal means to guarantee compliance with provisions of laws and regulations in the area of personal data protection.

The PDPB is empowered to enforce those provisions of the PDPA that are of an administrative nature, under the PDPA and the Administrative Regulation 42/2023. Criminal cases are reported to, and handled by, the Public Prosecutor's Office.

Administrative offences

To start proceedings relating to alleged violations, the PDPB must first take into account the actions of the alleged infringers, including the type of action and the intention of the agent, under the general administrative standards. Non-compliance with the special security measures required by Article 16 of the PDPA – for sensitive data processing and for the creation and maintenance of records regarding suspicion of illegal

activity, criminal offences and administrative offences – is an administrative offence which may entail a fine between MOP4,000 and MOP40,000.

Although the PDPA provides penalties for undue access, as well as for tampering with, or destruction of, personal data, it does not specifically provide for security breaches by the data controller. It should be noted, however, that the PDPA mandates that the data controller shall present the notification/authorisation request with a general description of the security measures, so that the PDPB may evaluate the adequacy of such measures. If the PDPB notifies the above-mentioned entity to address any insufficiency in the security measures and no remedy is taken, then a fine of between MOP2,000 and MOP20,000 for individuals and of between MOP10,000 and MOP100,000 for legal persons may be imposed. Other potential enforcement penalties are outlined below.

Non-compliance with notification of data processing in breach of the terms set out in Article 23 of the PDPA, providing false information after notification by the PDPB and maintaining access to open data transmission networks for data controllers which do not comply with the provisions of the PDPA are all punishable by administrative sanction. This will take the form of a fine between MOP2,000 and MOP20,000 for individuals and of between MOP10,000 and MOP100,000 for legal persons; the fines are increased to twice the amount indicated above if the data is subject to previous authorisation.

Non-compliance with stipulations of the PDPA regarding:

- data quality (Article 5);
- right to information, access, objection, right not to be subject to automated individual decisions (Articles 10 to 13);
- special security measures (Article 16);
- processing by subcontractor (Article 17); and
- non-provision of mandatory information provided in Article 24, paragraph 1,

involve an administrative sanction of a fine between MOP4,000 and MOP40,000.

Non-compliance with stipulations of the PDPA regarding:

- conditions for legitimacy of data processing (Article 6);
- processing of sensitive data (Article 7);
- suspicions of illegal activities, criminal offences and administrative offences (Article 8);
- interconnection of personal data (Article 9); and
- transfer of data to a destination outside the MSAR and respective exemptions (Articles 19 and 20),

involve an administrative sanction of a fine between MOP8,000 and MOP80,000.

Criminal offences

Non-compliance with stipulations of the PDPA regarding:

- purposefully omitting the notification/authorisation indicated in Articles 21 and 22 of the PDPA;
- providing false information in the notification/authorisation requests for the processing of personal data or making modifications in this request not allowed by the instrument of legalisation;
- diverting or using personal data, in a manner incompatible with the purpose of the collection or with the instrument of legalisation;
- promoting or carrying out an illegal interconnection of personal data;
- non-compliance with the obligations provided for in this law or in other data protection legislation in the period established by the PDPB; and
- maintaining access to open data transmission networks for those responsible for the processing of personal data that do not comply with the provisions of the PDPA, after notification of the PDPB not to do so,

involve a criminal sanction of imprisonment up to one year or a fine up to 120 days. Fines which are set in days are under the discretion of the court – each day's fine corresponds to an amount between MOP50 and MOP10,000, which the court shall set according to the economic and financial situation of the convicted person and their personal expenses. The sanction is increased to twice the duration indicated above if the data involved is sensitive (Article 7 of the PDPA) or if

illegal activities, criminal offences and administrative offences are suspected (Article 8 of the PDPA).

Access in any way to personal data whose access is forbidden to said individual/entity is forbidden. The sanction is increased to twice the duration indicated when access:

- is achieved through violation of technical safety rules;
- has allowed the agent or third parties to obtain personal data; or
- has provided the agent or third parties with a benefit or patrimonial advantage.

Such access is punishable with a criminal sanction of imprisonment up to one year or a fine up to 120 days, unless otherwise provided by special law. The sanction is increased to twice the duration indicated in the cases provided.

Deletion, destruction, damaging, suppression or modification of personal data without proper authorisation, rendering the data unusable or affecting its ability to be used is punishable with a criminal sanction: imprisonment up to two years or a fine up to 240 days, unless otherwise provided by special law. The sanction is increased to twice the duration indicated if the damage resulting therefrom is particularly serious. If the agent acts with negligence, the sanction is, in both of the cases provided above, imprisonment for up to one year or a fine up to 120 days.

Qualified disobedience regarding notification to interrupt, cease or block the processing of personal data, or in cases of:

- refusal, without just cause, to co-operate as specifically requested by the PDPB;
- refusal to totally or partially destroy personal data; and/or
- refusal to destroy personal data, after the period of conservation provided for in the PDPA,

involve a criminal sanction of imprisonment for up to two years or a fine up to 240 days.

1.9 Enforcement Trends

According to the two most recent annual reports published by the PDPB, in 2023 there were 105 investigations, mostly involving (in 55% of the cases) lack of legitimacy conditions for processing personal data or non-compliance with personal data protection principles (in 47% of the cases). In 2024, the number of investigations dropped to 74, involving lack of legitimacy in 66% of the cases and non-compliance with principles in 38% of the cases. The proportion of PDPB's own-motion investigations is low – 9% in 2023 and under 2% in 2024.

The investigations resulted in enforcement of penalties (fines) in 25% and 17% of the cases, in 2023 and 2024, respectively.

2. Privacy Litigation

2.1 Privacy Litigation Overview

The PDPA provides, in Article 14, that any person who has suffered damage as a result of an unlawful processing operation or of any other act incompatible with legal provisions or regulations in the area of personal data protection is entitled to receive compensation from the controller for the damage suffered. However, no case law exists on the basis of this provision.

2.2 Recent Case Law

No recent case law exists regarding Article 14 of the PDPA.

2.3 Collective Redress Mechanisms

There is no collective redress mechanism for protection of the collective interests of data subjects in Macau. As mentioned in **2.1 Privacy Litigation Overview**, individuals may file for damages arising from unlawful processing of their personal data. These cases are judged by the civil courts.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Macau has not enacted laws relating to processing of non-personal data.

The PDPA may apply where data processed may relate to an identified or identifiable natural person.

3.2 Interaction of Data Regulation and Data Protection

Macau has not enacted laws relating to processing of non-personal data.

3.3 Rights and Obligations Under Applicable Data Regulation

Macau has not enacted laws relating to processing of non-personal data.

3.4 Regulators and Enforcement

Macau has not enacted laws relating to processing of non-personal data.

4. Sectoral Topics

4.1 Use of Cookies

Cookies that are strictly necessary for the operation of a website may be lawfully used without any special requirements, under Article 6 of the PDPA.

Other cookies may only be used with the consent of the data subject.

In respect of other categories of personal data, the data subject has the right to be informed of the purposes of the cookies, the recipients or categories of recipients, and whether accepting cookies is obligatory or voluntary, as well as the possible consequences of rejecting the cookies. The controller must ensure that consent is freely given, specific and informed.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised advertising involves gathering information about the data subject.

As a minimum, upon collection of the relevant personal data, the data subject must be informed that their data may be used for the purpose of selecting goods or services that will be advertised to them later. Online marketing or any other form of direct marketing is subject to the provision of Article 12 (2) of the PDPA: The data subject has the right to object, on request

and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing or any other form of commercial research, or to be informed before personal data is disclosed for the first time to third parties for the purposes of direct marketing or for use on behalf of third parties, and to be expressly offered the right to object free of charge to such disclosure or uses.

Advertisers should also take into account the provisions of Law No 7/89/M, as republished by Law No 26/2024 (Advertising activity), restricting some practices and the advertising of some goods and services in Macau.

4.3 Employment Privacy Law

Labour relations in Macau are regulated by Law No 7/2008.

Article 8 (Protection of privacy) stipulates that (i) the employer and the employee should mutually respect each other's personal rights, in particular, the rights to protect the privacy of their personal lives and (ii) the right to privacy relates to access to and disclosure of information relating to the private and personal lives of either party, such as their respective family life, emotional and sexual lives, state of health and their political and religious convictions.

On the other hand, the PDPA stipulates, in Article 7 (1) (Sensitive data) that the processing of personal data revealing (...) trade-union membership (...) shall be prohibited.

Exceptions to this are provided in the case where:

- the data subject has given his explicit consent for such processing (Article 7 (2 (3))); and
- it is carried out with the data subject's consent in the course of its legitimate activities by a legal person or non-profit seeking body with a (...) trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to a third party without the consent of the data subjects.

Therefore, processing of trade union membership data is lawful in those two circumstances.

The duty of the employer to notify the PDPB of the processing of personal data of their employees is waived in some cases:

- personal data necessary for processing of payroll and payroll-related obligations (Authorisation No 01/2007);
- personal data necessary for processing of administrative management of the employment relation (Authorisation No 02/2007); and
- processing of biometric data for attendance control purposes (Authorisation No 02/2020).

The PDPB provides detailed recommendations on the use of personal data for supervision of employees' activities in the workplace, emphasising the principles of legality of purpose, non-excessive collection and including sample privacy statements for processing of supervision of telephone calls, e-mail and internet usage and video surveillance.

4.4 Data Protection in M&A

In asset deals, the standard provisions of the PDPA apply. Namely, the buyer, as a recipient for the personal data controlled by the seller, shall become the controller of the data.

The data subjects' right to information includes the identity of the recipients and the purposes of the disclosure of data to those recipients.

Besides, the identity and purposes of processing of the recipients are part of the notification to the PDPB and this notification might also need to be amended/updated.

The recipient must fulfil the requirements of legitimacy for processing the transferred data.

Therefore, either consent from the data subjects or another condition for legitimacy needs to be secured, along with a notification to the PDPB, whenever the processing is not already covered by such a notification.

5. International Considerations

5.1 Restrictions on International Data Transfers

The transfer of personal data overseas can only take place in accordance with PDPA provisions and provided that the jurisdiction to which the data is going to be transferred ensures an adequate level of protection.

This level of protection may be assessed by the PDPB on a case-by-case basis (Article 19 of the PDPA) but, in practice, the PDPB does not assess the adequacy of the level of protection guaranteed by the import jurisdiction.

All cases are assessed under Article 20 of the PDPA on derogations (see below).

Under the PDPA there is no provision enabling the publication of a list of jurisdictions capable of ensuring the level of protection that is imposed by the PDPA (no "white list").

The transfer of data overseas may be possible under the various exceptions provided by the PDPA.

These include the necessity of such a transfer for the formation of a contract between the data subject and the data controller and for preliminary measures for the formation of that contract at the request of the data subject, among others.

However, the most common exception to the rule indicated above is the obtaining of the data subject's express and unambiguous consent to such a transfer (Article 20, paragraph 1 of the PDPA).

Organisations collecting or transferring data in connection with foreign government data requests, foreign litigation proceedings (eg, civil discovery) or internal investigations are not exempted from the standard requirements set out under the PDPA and shall be subject to the same penalties in case of breach of the existing laws.

5.2 Government Notifications and Approvals

As no list of jurisdictions ensuring an adequate level of protection currently exists in Macau, the transfer

of personal data abroad is subject to prior authorisation by the PDPB, as indicated in **5.1 Restrictions on International Data Transfers**.

If express and unequivocal consent from the data subject is obtained, or if the situation under analysis falls under one of the exceptions provided by the PDPA, a simple notification is sufficient and complies with the legal provisions.

5.3 Data Localisation Requirements

The international transfer of data is subject to the requirements referred to in **5.1 Restrictions on International Data Transfers**.

5.4 Blocking Statutes

This issue does not arise in the Macau SAR jurisdiction.

5.5 Recent Developments

The PDPB, jointly with the Economic and Technological Development Bureau (DSED) and the Cyberspace Administration of China, continue to develop the implementation of the “Standard Contract for cross-border flow of personal information in the Greater Bay Area Guangdong-Hong Kong-Macau (Mainland China – Macau)”, launched in September 2024.

Trends and Developments

Contributed by:

Pedro Cortés and Luís Rôlo

Lektou – Advogados e Notários

Lektou – Advogados e Notários is a Macau SAR-based law firm with more than 35 years' experience of legal practice. Services regularly provided by the firm include advising on Macau law, helping international companies start their businesses in Macau, and assisting in the reorganisation of economic groups with connections to Macau. In 2016, Lektou partnered with Zhong Yin Law Firm (People's Republic of China – PRC) and Fongs (Hong Kong) to open a new office in Hengqin Island, Zhuhai, PRC – ZLF Law

Firm. This was the first law office to unite firms from the two Special Administrative Regions and Mainland China. Since then, it has extended and opened an office in Shenzhen. In 2017, Lektou extended its operations to Lisbon, Portugal, through a locally based law firm, Rato & Cortés, as part of its internationalisation strategy to position itself as a legal player in the platform between the PRC and Portuguese-speaking countries.

Authors



Pedro Cortés is managing partner of Lektou, where he initiated his career as a lawyer in 2003, with experience in gaming, corporate and M&A, capital markets, and banking and finance. He is admitted to practise

law in Macau, Portugal, Brazil (São Paulo), China (as a cross-border Macau lawyer) and in East Timor. He is a member of the International Association of Gaming Advisors (IAGA), the Hong Kong Institute of Directors (HKIoD), International Masters of Gaming Law (IMGL), the International Bar Association (IBA), the Chartered Institute of Arbitrators (CI Arb) and the Hong Kong Institute of Arbitrators (HKIA). Pedro is a guest lecturer at the Portuguese Catholic University – Lisbon School of Law, and of the Autónoma Academy in Lisbon.



Luís Rôlo is currently a trainee lawyer with Lektou, having joined the firm in 2020. He graduated from the University of Macau in 2008 and is registered with the Macau Lawyers Association. His professional

background includes being a senior officer at the Macau Pension Fund (1988–99), a senior officer at the Financial Services Bureau (1999–2010), a jurist at the Cabinet of the Commissioner Against Corruption (2010–14) and a jurist at the Office for Personal Data Protection (2014–18).

Lektou – Advogados e Notários

Avenida da Amizade, 555
Landmark Office Tower
23rd Floor
Macau SAR

Tel: +853 2856 2322
Fax: +853 2858 0991
Email: mail@lektou.com
Web: www.lektou.com



Legal Framework

The Personal Data Protection Act of Macau (PDPA) was enacted by Law No 8/2005, and follows very closely the text of the former Portuguese Act of 1998, with the notable exception of the provisions on the Public Authority for Personal Data Protection.

The Act on Video Surveillance in Public Areas was enacted by Law No 2/2012.

The Personal Data Protection Bureau (PDPB) is the public authority with regulatory and supervisory powers, created in 2023 by Administrative Regulation No 42/2023. It succeeded the former Office for Personal Data Protection (OPDP).

The PDPB is a permanent Bureau of the Public Administration of the Macau Special Administrative Region, and, despite not having a formal independent status, it is placed under the direct authority of the Chief Executive, not under a Secretary of the Government.

This means that the PDPB is not under the authority of other public administration bodies in the performance of its regulatory and supervision powers.

The PDPB is an Observer to the Global Privacy Assembly.

The substantive law framework has not seen a significant change in the last few years, and no plans to legislate in the field of Personal Data Protection have been announced.

The previously reported concerns, namely regarding a duty of notification of data breaches to the data subjects, provision for mandatory privacy officers in relevant controllers, preliminary assessments of impact on privacy to be carried out by large-scale controllers, duties in connection to further transfers in the case of cross-border transfer of personal data, remain current.

The continued expansion of AI is an additional challenge to the resilience of the PDPA.

Another area where the Macau SAR may consider a revision of the legal framework is the requirement for

notification (registration) of processing of personal data with the PDPB.

This notification is an administrative requirement, not necessarily followed by an assessment of the lawfulness of the notified processing of personal data.

The volume of such notifications remained high in 2023 and 2024, with more than 1,500 cases each year.

It is debatable whether the benefits of this system outweigh the administrative burden it imposes.

The challenges posed by AI tools and their impact on privacy and personal data protection are being addressed worldwide and one may expect that the new PDPB will address them, either by issuing guidelines or by promoting legislation and/or regulation on the subject.

Enforcement

The PDPB will continue to publish annual reports of activity, offering some insight on its approach to enforcement. Two distinct phases have been observed in this regard in the past.

- During the first few years of operation, the OPDP provided for the education of the public, conducting a variety of activities intended to foster the awareness of rights and obligations both of data subjects and controllers regarding privacy issues.
- More recently, the priority has shifted somewhat towards enforcement and this is shown both in the number of investigations conducted and in the number of penalties applied; this is most notable in the field of direct marketing or telemarketing.

2024 did not show a significant trend for change in the average number of new investigations (74, compared to 105 in 2023 and 73 in 2022) and in the number of sanctions applied (14 offenders, compared to 30 in 2023 and 18 in 2022).

Less than 2% of the investigations were own-motion.

Transfer of Personal Data to Jurisdictions outside Macau – “White List”

There were no recent developments on this subject.

The apparent provision of Article 19 of the PDPA for adopting a white list of jurisdictions for the purpose of cross-border data transfers does not translate into a practicable mechanism.

The PDPB is expected to continue to solve this problem by resorting in every case to Article 20 of the PDPA (Derogations), which allows for transfers, even where “the legal system does not ensure an adequate level of protection”, provided that “the data subject has given his consent unambiguously to the proposed transfer” and in a number of other limited circumstances (as per Article 20 of the PDPA).

Any change to this situation depends of the amendment to the relevant provisions of the PDPA.

In respect of regional cross-border data flows, there is a close co-operation with the Cyberspace Administration of China, for facilitating the flow of personal information in the context of the Greater Bay Area Guangdong-Hong Kong-Macau.

In a joint initiative, together with the Economic and Technological Development Bureau of Macau (DSED) and the Cyberspace Administration of China, the PDPB launched the “Standard Contract for cross-border flow of personal information in the Greater Bay Area Guangdong-Hong Kong-Macau (Mainland China – Macau)”.

Data Combination (Interconnection)

The PDPA subjects the processing of personal data involving “data combination” to prior checking and authorisation by the OPDP. It also makes it a criminal offence to “promote or carry out an illegal combination of personal data”, punishable with imprisonment for a period not exceeding one year or a fine not exceeding 120 days (double maxima if sensitive data is involved). This would be the case should the controller fail to secure the authorisation.

In practice, almost every department of the public administration is empowered, by law or by its organic regulation, to conduct data combination in areas related to their lawful activities.

There is a tight connection between this topic and the development of e-Government, making the use of data combination by the public administration the norm, rather than the exception.

However, in the private sector, the need for securing a prior authorisation from the OPDP, keeps the processing by means of data combination as an exception.

The total number of applications for authorisations (mostly granted to bodies of the public sector, including data combination) was 48 in 2024, compared with 57 in 2023 and 33 in 2022.

Video Surveillance

Macau’s video surveillance programme, “Eyes in the Sky”, continues to develop.

As the initial phases have yielded satisfactory results in criminal investigation, the authorities have disclosed plans to further expand the system, which is expected to include up to 4,200 cameras by 2028.

The system has the capability to provide facial recognition and vehicle licence plate recognition.

In respect of the retention period of the collected data, the authorities have stated that, under normal circumstances (ie, if no criminal investigation is involved), all the data is automatically erased 60 days after collection.

Under the 2012 Act, the OPDP’s prior opinion is required for each camera, regarding the location, the angle of coverage and its width of field. The OPDP regularly confirms that this has been carried out. However, the particulars of the process are not disclosed to the public.

PIPL

Mainland China’s Personal Information Protection Law (PIPL) has a special significance for Macau, given the intense economic and human cross-border flows.

The PDPB continues to engage in joint activities with the Commissioner of the Office of the Privacy Commissioner for Personal Data, Hong Kong and the Cyberspace Administration of China, among others.

The PDPB is expected to continue promoting multiple awareness actions to ensure that local operators are in compliance with the PIPL requirements.

e-Government

Macau has introduced a growing number of e-Government services, covering multiple areas of the administrative procedures of the residents.

The different services are being brought together into a unified platform, the “Macau One Account” making them available online via mobile phone.

This has been developed to enable residents to produce a growing list of documents (eg, ID, driver’s licence) only by exhibiting their digital version.

The processing of the relevant personal data is subject to the PDPA. As a number of e-services require the combination of data held by two or more different public departments, the organic regulations of these departments, some specific acts or PDPB authorisations, provide the legal grounds for such combination.

The trend for expanding the “Macau One Account” platform is likely to continue over the near future.



Law and Practice

Contributed by:

Deepak Pillai, Yong Shih Han and Matthew Chang Jun Xiang
Christopher & Lee Ong

Contents

1. Legal and Regulatory Framework p.287

- 1.1 Overview of Data and Privacy-Related Laws p.287
- 1.2 Rights and Obligations p.288
- 1.3 Special Categories of Personal Data p.289
- 1.4 Processing of Personal Data for Research and Development Purposes p.289
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.290
- 1.6 Data Breach Requirement p.291
- 1.7 Regulators p.292
- 1.8 Enforcement Proceedings and Fines p.292
- 1.9 Enforcement Trends p.293

2. Privacy Litigation p.293

- 2.1 Privacy Litigation Overview p.293
- 2.2 Recent Case Law p.294
- 2.3 Collective Redress Mechanisms p.295

3. Requirements for the Protection and Processing of Non-Personal Data p.295

- 3.1 Objectives and Scope of Data Regulation p.295
- 3.2 Interaction of Data Regulation and Data Protection p.296
- 3.3 Rights and Obligations Under Applicable Data Regulation p.297
- 3.4 Regulators and Enforcement p.297

4. Sectoral Topics p.297

- 4.1 Use of Cookies p.297
- 4.2 Personalised Advertising and Other Online Marketing Practices p.298
- 4.3 Employment Privacy Law p.299
- 4.4 Data Protection in M&A p.300

5. International Considerations p.300

- 5.1 Restrictions on International Data Transfers p.300
- 5.2 Government Notifications and Approvals p.301
- 5.3 Data Localisation Requirements p.301
- 5.4 Blocking Statutes p.301
- 5.5 Recent Developments p.301

Christopher & Lee Ong (CLO) is located in Kuala Lumpur where it has a 25-practitioner strong TMT practice – the largest in Malaysia – which leads the Malaysian TMT legal landscape in terms of the range, breadth and depth of the legal services offered to clients. CLO advises major multinational corporations and conglomerates across banking, insurance, technology and telecommunications, and has done so for several decades. The firm also handles fintech, e-commerce, e-health and electric vehicles matters, as well as online media and content. The firm has seen

a steady increase in data centre and AI-related work, advising foreign operators establishing data centres in Malaysia and the ASEAN region, often alongside telecoms, corporate and tax considerations. CLO also regularly acts for global software giants that actively engage the firm as part of the Rajah & Tann Asia Network. In addition, the firm receives frequent instructions from European clients on Malaysian law in the context of GDPR compliance and cross-border data transfers.

Authors



Deepak Pillai heads CLO's TMT and data protection practice group and has practised in technology, telecommunications and data protection law since 1997. He advises international, private and public

sector clients on IT and cloud contracts, electronic commerce, online financial services, outsourcing, telecoms, cybersecurity, data protection, AI and online content, including in complex regulatory, policy and legislative matters. Deepak has been consistently recognised by leading legal directories since 2001, and is ranked in Band 1 for TMT in the Chambers Asia-Pacific Guide 2026. He also serves on the PDPA Appeals Tribunal and the Malaysian Bar's PDPA Committee.



Matthew Chang Jun Xiang is an associate in the technology, media and telecommunications and data protection and privacy practice group of CLO. He regularly assists with technology-related contracts,

including contracts relating to the implementation of IT systems, software development and subscription, maintenance and support, as well as service levels. Matthew also advises on data protection and cybersecurity clauses within IT contracts, including for clients operating within regulated sectors.



Yong Shih Han is a partner in CLO's technology, media and telecommunications and data protection practice group. She has been recognised by legal directories as an up-and-coming figure in TMT.

She regularly advises clients on a wide range of matters relating to information and communications technology, information security and data protection, telecommunications, and media and advertising laws. Her work includes drafting and advising on technology-related contracts and policies, regulatory and compliance matters, and issues that may lead to dispute resolution.

Christopher & Lee Ong

Level 22 Axiata Tower
No 9 Jalan Stesen Sentral 5
Kuala Lumpur Sentral
50470 Kuala Lumpur
Malaysia

Tel: +603 2273 1919
Fax: +603 2273 8310
Email: clo-info@christopherleeong.com
Web: www.christopherleeong.com

**Christopher
& Lee Ong**
Malaysia

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

In Malaysia, the data protection and privacy law is provided for in the federal constitution as well as in a dedicated act of parliament governing the collection of personal data in the context of commercial transactions.

Federal Constitution

The federal constitution of Malaysia does not expressly list privacy as a fundamental right. However, Malaysian case law has, in limited circumstances, interpreted the right to life and personal liberty under Article 5 (1) as encompassing a right to privacy.

Personal Data Protection Laws in Malaysia

The Personal Data Protection Act 2010 (PDPA) acts as the primary legislation governing the collection and processing of personal data in commercial transactions. In line with that, the Personal Data Protection Commissioner (the “Commissioner”) and the Department of Personal Data Protection (*Jabatan Perlindungan Data Peribadi* or JPDP) were established to implement and enforce the PDPA.

Since the PDPA came into force, several subsidiary regulations and guidelines have been introduced, including:

- the Personal Data Protection Regulations 2013 (PDP Regulations);

- the Personal Data Protection (Class of Data Users) Order 2013;
- the Personal Data Protection (Registration of Data User) Regulations 2013;
- the Personal Data Protection Standard 2015 (PDP Standard);
- the Guide to Prepare Personal Data Protection Notice 2022; and
- the General Code of Practice of Personal Data Protection.

Pursuant to the Personal Data Protection (Amendment) Act 2024 (the “Amendment Act”), a suite of guidelines have been, or will be issued by the Commissioner. These include, namely:

- the Data Breach Notification Guideline (“DBN Guideline”) (issued 25 February 2025);
- the Appointment of Data Protection Officer Guideline (“DPO Guideline”) (issued 25 February 2025);
- the Right to Data Portability Guideline (“Data Portability Guideline”);
- the Cross Border Data Transfer Guideline (“CBDT Guideline”) (issued 29 April 2025);
- the Management of Data Protection Officer Training Service Providers Guideline (issued 21 July 2025);
- the Data Protection Officer Competency Guideline (issued 21 July 2025);
- the Data Protection Officer Professional Development Pathway & Training Roadmap (issued 21 July 2025);
- the Data Protection Impact Assessment Guideline;

- the Data Protection by Design Guideline (“DPbD Guideline”); and
- the Automated Decision Making and Profiling Guideline (“ADMP Guideline”).

In addition to the above guidelines, sector-specific codes of practice have also been developed, including for banking and financial services, healthcare, and the aviation sector. These codes set out additional obligations tailored to the operational circumstances of each sector and industry.

Sector-Specific Requirements

In addition to the PDPA, there are data protection requirements prescribed by sector-specific regulations. For example, in the banking and financial sector, Section 133 of the Financial Services Act 2013 (FSA) imposes secrecy obligations, except where one of the conditions for permitted disclosure is met. Bank Negara Malaysia (BNM)’s Risk Management in Technology (RMiT) policy document requires financial institutions to establish comprehensive cyber crisis management frameworks, including a cyber-incident response plan. The Management of Customer Information and Permitted Disclosures (MCIPD) policy document further prescribes detailed measures and controls governing the collection, storage, use, transmission, sharing, disclosure and disposal of customer information.

Data Sharing Between Public Sector Agencies

Where personal data is shared between federal public sector agencies, the Data Sharing Act 2025 (DSA) applies. The DSA imposes statutory duties on public sector agencies that request or provide data to other agencies, including requirements to take appropriate measures to safeguard the security and confidentiality of the data, maintain records of the shared data, and report any unauthorised disclosure to the Director General of the National Digital Department (DGND).

Taken as a whole, Malaysia’s data governance framework operates on a layered basis. The PDPA governs private-sector processing of personal data in commercial contexts, supplemented by sector-specific regulatory instruments and codes of practice.

1.2 Rights and Obligations

Data controllers (ie, persons who process personal data or have control or authority over the processing of personal data) are required to comply with the relevant requirements under the PDPA. This includes the requirement to comply with the seven personal data protection principles (“PDP Principles”), namely:

- General Principle (Section 6) – this is the general requirement to obtain the consent of data subjects for the processing of their personal data, unless any of the PDPA exemptions apply. Additionally, the processing of personal data must be for a lawful purpose directly related to the data controller’s activities and be adequate, relevant and not excessive in relation to that purpose. Finally, where sensitive personal data is involved, data controllers are required to obtain the explicit consent of the data subject unless one of the relevant exemptions under Section 40 applies;
- Notice and Choice Principle (Section 7) – this is the requirement to issue a written privacy notice in both Bahasa Malaysia and English, setting out the relevant information required under Section 7 of the PDPA;
- Disclosure Principle (Section 8) – this is the prohibition from the disclosure of personal data without the data subject’s consent, except where the disclosure is for purposes or to parties specified in the data controller’s privacy notice, or where an exemption under the PDPA applies;
- Security Principle (Section 9) – this is the requirement to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard to the matters specified in the PDPA;
- Retention Principle (Section 10) – this is the obligation to only retain personal data for the period necessary to achieve the purpose for which it was collected and processed, and to destroy or permanently delete such data when it is no longer needed;
- Data Integrity Principle (Section 11) – this is the requirement to take reasonable steps to ensure that personal data is accurate, complete, not misleading, and kept up to date; and

- Access Principle (Section 12) – this is the requirement to allow data subjects to access and correct their personal data.

In addition to the seven principles, the PDPA also prohibits the transfer of personal data outside Malaysia, unless one of the conditions listed under Sections 129 (2) or (3) of the PDPA is met.

With respect to data subject rights, the PDPA confers data subjects with several rights in respect of their personal data:

- right of access to personal data – data subjects are entitled to be informed by a data controller as to whether their personal data is being processed by, or on behalf of the controller;
- right to correct personal data – data subjects are entitled to correct their personal data if it is inaccurate, incomplete, misleading or out of date;
- right to withdraw consent – data subjects are entitled to withdraw their consent to the processing of their personal data;
- right to prevent processing of personal data that is likely to cause damage or distress – data subjects are entitled to request that the data controller cease or not commence the processing of their personal data based on the reasons that the processing is causing or is likely to cause substantial damage or substantial distress to the data subject or another person, and such damage or distress is or would be unwarranted;
- right to prevent processing for purposes of direct marketing – data subjects are entitled to request that the data controller cease or not commence the processing of their personal data for direct marketing purposes; and
- right to data portability – data subjects are entitled to request that the data controller transmit their personal data directly to another data controller, subject to technical feasibility and compatibility of format.

1.3 Special Categories of Personal Data

Under the PDPA, any personal data relating to the physical or mental health of a data subject, their political opinions, religious beliefs or other similar beliefs, biometric data, or the commission or alleged com-

mission of an offence, is considered to be “sensitive personal data”.

As a general rule, explicit consent is required for the processing of sensitive personal data. While the PDPA does not provide any definition or guide as to what constitutes explicit consent, it is generally understood that explicit consent requires the data subject to have carried out an affirmative action to signify their consent. This includes:

- writing the words “I consent”;
- ticking a check box; or
- providing their signature.

Both data controllers and data processors (ie, any person who processes personal data for and on behalf of a data controller, and not for its own purposes) are required to implement enhanced security safeguards to protect sensitive personal data. This is because under the PDPA’s Security Principle, the level of security should correspond to the nature of the personal data and the harm that may result from its loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Processing of Personal Data of Children

The PDPA does not impose children-specific data protection obligations. Nevertheless, as individuals below the age of 18 are not legally able to provide consent, Regulation 3 (3) of the PDP Regulations provides that consent for the processing of a child’s personal data must be obtained from a parent, guardian, or any such person with parental responsibility over that child.

1.4 Processing of Personal Data for Research and Development Purposes

When personal data is processed for the purpose of preparing statistics or carrying out research, the processing is exempted from the General, Notice and Choice, Disclosure and Access Principles, as well as other related provisions of the PDPA. This exemption applies only where the personal data is not used for any other purpose and the resulting statistics or research findings are anonymised, such that no data subject is identifiable.

Additionally, the Commissioner intends to issue the DPbD Guideline which aims to encourage data controllers to integrate privacy considerations into all aspects of their personal data management. Based on the Public Consultation Paper on the DPbD Guideline, the DPbD Guideline intends to introduce the element of data minimisation, which encourages data controllers to verify whether the relevant purposes for processing personal data can be achieved by using less detailed, aggregated, or non-personal data. Where the purpose ultimately does not require identification – such as in statistical analyses – the DPbD Guideline expects controllers to delete or anonymise personal data as soon as identification is no longer required. If identification must be retained for other processing activities, controllers are encouraged to apply pseudonymisation to reduce the risk to data subjects.

Sector-Specific Requirements

Similarly, the Malaysian Medical Council's Guidelines on Confidentiality echo this principle by ensuring that data used for medical research or audit be anonymised wherever practicable. Where anonymisation is not feasible or would undermine the validity of the research, the Guidelines on Confidentiality require that express consent be obtained before any identifiable patient data is used or disclosed. This reflects a consistent approach in Malaysia where anonymisation is preferred for research purposes, and identifiable data may be used only where necessary and with appropriate safeguards.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Malaysia currently does not have a dedicated statute or comprehensive regulatory framework governing AI. As a result, the legal landscape is shaped primarily by non-binding policy guidelines and the application of existing laws to AI-related activities. While certain sectoral regulators have introduced guidelines or requirements to address AI risks within their respective domains, such initiatives remain limited in scope and are the exception rather than the rule.

In the absence of binding AI-specific legislation, reference is often made to the National Guidelines on AI Governance and Ethics ("NAIGE"). While NAIGE does not carry any legal effect, it currently serves as

Malaysia's principal policy instrument for promoting responsible and ethical AI development and use. NAIGE sets out seven AI principles that end users, including individuals and organisations deploying AI systems, are expected to observe. One of the key principles is "privacy and security", which emphasises that when handling personal data such as financial or health information, proper procedures, informed consent, and secure storage practices are essential. In line with this, NAIGE underscores the need for robust security measures to protect against hacking, data breaches and other malicious activities.

Therefore, AI developers are encouraged to obtain consent where required, ensure privacy and data protection throughout the AI system life cycle, avoid unlawful or discriminatory use of data, and incorporate privacy-by-design and security-by-design approaches aligned with relevant international standards.

Separately, the Commissioner intends to issue the ADMP Guideline to address risks arising from the use of automated systems. Based on the public consultation paper on the ADMP Guideline, the guideline intends to confer three rights on data subjects, collectively referred to as the Automated Decision-Making Restrictions:

- the right to refuse to be subjected to a decision based solely on automated decision-making (including profiling) which produces legal effects concerning the data subjects or significantly affects the data subject;
- a right to information on the automated decision-making being undertaken (ie, the transparency requirement); and
- a right to request a human review of the automated decision-making.

In addition, the public consultation paper on the ADMP Guideline highlights the Commissioner's proposal to introduce specific safeguards for the processing of biometric data in the context of automated decision-making and profiling. However, as automated decision-making and profiling are not currently recognised or defined concepts under the PDPA, it remains to be seen whether the ADMP Guideline, once issued, will carry any binding legal effect.

1.6 Data Breach Requirement Notification Requirement and Timeline

The PDPA read in line with the DBN Guideline imposes a requirement on data controllers to notify the Commissioner of the occurrence of a personal data breach if the personal data breach causes, or is likely to cause, “significant harm” to data subjects or is of a “significant scale”. A personal data breach is considered to be of a “significant scale” where it affects more than 1,000 data subjects.

On the other hand, “significant harm” includes instances where there is a risk that the compromised personal data:

- may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;
- may be misused for illegal purposes;
- consists of sensitive personal data; or
- consists of personal data and other personal information which, when combined, could potentially enable identity fraud.

Notification must be made as soon as possible and no later than 72 hours from the occurrence of the breach. If the data controller is unable to submit the notification to the Commissioner within 72 hours, the data controller must submit a written notice to the Commissioner detailing the reasons for the delay, together with supporting evidence.

Besides the Commissioner, data controllers must also notify affected data subjects if a breach results in, or is likely to result in, “significant harm” to the affected data subjects. Affected data subjects must be notified of the personal data breach without unnecessary delay and in any case, no later than seven days after the initial data breach notification is made to the Commissioner.

Dealing With the Data Breach

The DBN Guideline imposes a requirement on data controllers to act promptly as soon as they become aware of any personal data breach by assessing, containing and reducing the potential impact of the data breach, by considering the following immediate containment actions where applicable:

- isolate and disconnect the compromised database or system from the network;
- suspend or disable compromised access rights;
- stop the practices identified as having caused the data breach; and
- determine whether the lost data can be recovered or whether any immediate remedial action can be taken to minimise further harm being caused by the breach.

Data controllers are also required to conduct a post-breach evaluation to review the effectiveness of the data breach management and response plan, as well as its data protection practices and policies to prevent the recurrence of similar incidents.

In addition, data controllers are required to keep and maintain written records and a register detailing all occurrences of personal data breaches for a period of at least two years from the date of notification to the Commissioner.

Individual Claims

The PDPA does not expressly allow aggrieved claimants to pursue civil actions against data controllers for any breach of the provisions of the PDPA including for any loss or damage arising from a personal data breach. This position was affirmed in the Court of Appeal case of *Ranjan Paramalingam & Anor v Persatuan Penduduk Taman Bangsar Kuala Lumpur* [2023] 1 MLJ 459. However, claimants may still initiate civil actions against data controllers through other causes of action, such as breach of contract for the data controller’s breach of its obligations to protect the aggrieved claimant’s personal data.

Sector-Specific Requirements

Certain sectors also impose data breach notification requirements. For example, Paragraph 11 of the MCIPD lays out the exact requirements financial institutions must comply with when dealing with customer information breaches. As notification of data breaches under the MCIPD is directed to BNM, the financial institution will also need to comply with the data breach notification requirements under the PDPA, and notify the JPDP within the prescribed timeframes.

1.7 Regulators

The Commissioner, assisted by officers in the JPDP, acts as the primary regulator overseeing enforcement of the PDPA and its regulations.

Section 48 of the PDPA lays out the functions of the Commissioner, which include:

- implementing and enforcing the PDPA;
- monitoring and supervising compliance with the PDPA; and
- promoting awareness and disseminating information to the public about the operation of the PDPA.

In addition to the general functions and powers, the Commissioner is provided with a wide range of investigative and enforcement powers, which include the power to:

- inspect any personal data system used by a data controller for the purpose of obtaining information that would assist the Commissioner in making recommendations to promote the data controller's compliance with the PDPA;
- carry out investigations where complaints have been lodged by data subjects or where the Commissioner has reasonable grounds to believe that a data controller may be in contravention of the PDPA;
- issue enforcement notices to direct a data controller to take steps to remedy any contravention of the PDPA, or to cease processing personal data until the contravention has been remedied;
- carry out search and seizure with or without a warrant on the data controller's premises;
- request access to computerised data when conducting a search on the data controller's premises;
- require production of any computer, book, account, computerised data or other document kept by the data controller;
- require attendance of persons acquainted with the case and examine such persons to obtain their statement when carrying out its investigation under the PDPA;
- arrest without warrant any person reasonably believed to have committed, or to be attempting to commit, an offence under the PDPA; and
- issue compounds for offences under the PDPA.

Note that the digital minister has proposed elevating the Commissioner's office, which currently operates as a government department, into a full-fledged independent data commission. This proposed reform aims to enhance the Commissioner's enforcement and oversight powers, and to strengthen overall data protection and governance in Malaysia.

Sector-Specific Requirements

In addition to the JPDP, regulators who oversee specific sectors are provided with the power to ensure compliance with specific sectorial requirements. For example, BNM acts as the regulator of the financial sector. It is provided with vast powers to oversee compliance with the FSA and set standards relating to the conduct of financial institutions, including conduct relating to the processing of customer information.

Data Sharing Between Public Sector Agencies

The DSA sets up the National Data Sharing Committee (NDSC), which oversees the implementation of the DSA. They are assisted by the DGNDD. Their roles are further discussed in **3.4 Regulators and Enforcement**.

1.8 Enforcement Proceedings and Fines Investigations and Enforcement Notices

The PDPA does not grant data subjects a private right of action or a right to claim compensation from data controllers or data processors for non-compliance with the PDPA. Instead, aggrieved individuals may lodge written complaints with the Commissioner in respect of any act, practice or request relating to their personal data. Upon receiving such a complaint, the Commissioner may conduct an investigation unless one of the circumstances under Section 106 of the PDPA applies, which permits the Commissioner to refuse to proceed with the complaint (eg, the complaint is frivolous, vexatious or is not made in good faith).

Following an investigation, the Commissioner may issue an enforcement notice to a data controller if he is of the opinion that the data controller is contravening any provision of the PDPA or has previously contravened it in circumstances that make it likely that the contravention may continue or be repeated. The enforcement notice will state the Commissioner's findings, identify the relevant statutory provision that has

been breached and direct the data controller to take specified steps to remedy the contravention within a prescribed period. The notice may also require the data controller to cease processing personal data pending the rectification of the breach.

Data controllers who are not satisfied or disagree with the enforcement notice may initiate appeal proceedings with the Appeal Tribunal. Failure to comply with an enforcement notice constitutes an offence, punishable by a fine of up to MYR200,000, imprisonment for up to two years, or both.

Penalties for Breaches

Data controllers are also reminded that various provisions of the PDPA carry fines and jail terms, with any contravention of the PDP Principles carrying a maximum fine of MYR1 million and/or imprisonment for up to three years.

Sector-Specific Requirements

Apart from the PDPA, data controllers in certain sectors may also be at risk of breaching certain sectoral requirements, such as Section 133 of the FSA. Any person who contravenes Section 133 of the FSA shall on conviction be liable to a fine not exceeding MYR10 million, five years' imprisonment or both.

Similarly, Section 234 of the FSA provides BNM with the power to take action against any person who has committed a breach under the FSA, or if the person has failed to comply with or give effect to any standards, such as the RMIT or MCIPD. This includes the power to prescribe monetary penalties as well as the power to provide the person with a notice in writing ordering them to comply or give effect to the standard.

Data Sharing Between Public Sector Agencies

Section 18 of the DSA provides that any officer or servant of a data recipient shall not use or disclose the data shared under the DSA other than for the purpose for which the data is shared.

1.9 Enforcement Trends

According to the list of inspection activities published on the JPDP's website, the JPDP carried out four inspection visits to four different data controllers' personal data systems, as well as two enforce-

ment activities against unregistered data controllers. The Commissioner also released a list of compound cases issued under the PDPA from 2017 to 2025, which recorded that a total of 33 data controllers were required to pay a compounded fee for breaches to one or more sections under the PDPA. Additionally, a total of eight cases were taken to court. To date, the highest publicly reported compound issued under the PDPA is MYR108,000 for breaches of the General, Disclosure and Retention Principles.

Based on the above trends, data controllers should place higher importance on ensuring their compliance with the PDPA including the seven PDP Principles, and ensure adherence to the PDP Standards, the PDP Regulations, and any subsidiary legislation or guidelines issued pursuant to the PDPA.

Sector-Specific Requirements

BNM has over the past years carried out various enforcement activities against financial institutions. The trend relating to enforcement activities for disclosing customer information is discussed under 3.4 **Regulators and Enforcement**.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Over the past 24 months, a small number of cases involving civil claims for non-compliance with the PDPA have been brought to court. However, these cases were dismissed, with the courts either making a finding that there was no breach, or that the PDPA did not provide data subjects with the ability to pursue civil claims on the basis of non-compliance with the PDPA.

On the other hand, the PDPA has been used in court to contend that certain documents should not be produced in court as this would violate the disclosure principle under the PDPA. These typically involved cases focused on disputes of a different nature, such as disputes over employment or banking which required the production of certain documents or personal data.

Finally, in a recent significant case, namely *Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors* [2025] 4 CLJ 710, the claimant commenced judicial review proceedings against a statutory body relating to disputes over the disclosure of personal data.

That said, the number of cases involving the PDPA since 2010 have been limited in number, often due to the fact that aggrieved parties are prevented from pursuing civil claims against the non-complying party. This is unlikely to change in the near future as the Commissioner of the JPDP has not signalled any intention to introduce civil claims and remedies under the PDPA. Therefore, future cases are likely to primarily involve the disclosure of documents or information as well as judicial review proceedings.

2.2 Recent Case Law

Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors

The case of *Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors* [2025] 4 CLJ 710 garnered a great deal of public attention as it was the first time that the director general of Inland Revenue was taken to court over a personal data-related dispute. As such, the case was touted to lay the groundwork for the extent to which a statutory body may request and obtain access to personal data.

Under the Income Tax Act 1967 (ITA), the Inland Revenue Broad of Malaysia (IRB) is provided with broad powers to ensure effective collection of tax revenue. This includes Section 81 of the ITA, which empowers the director general of the IRB (DGIR) to demand the disclosure of information or particulars that are in the possession or control of a person, for the purposes of the ITA.

The dispute arose when the DGIR exercised his powers under Section 81 of the ITA to demand that Genting Malaysia Berhad (“Genting”) disclose the personal data of all of its customers who were members under the Genting Rewards Loyalty Programme (“Loyalty Programme”) for the purposes of enlarging the IRB’s tax base.

Genting refused to agree to the demand, stating that complying with the DGIR’s demands would result in Genting breaching its obligations to customers under the PDPA. In response, the DGIR stated that the disclosure was permitted under the PDPA as it met the exemptions listed under Sections 39 and 45 of the PDPA. As a result of this, Genting subsequently filed a judicial review application with the High Court, which then ruled that the PDPA does not allow the DGIR to make blanket demands for personal data (in this case, the demand for the data of all customers who were members of the Loyalty Programme).

That said, the High Court’s ruling was overturned by the Court of Appeal, which ruled that the judicial review application brought forward by Genting was time barred as it was filed after the three-month window prescribed by Order 53 Rule 3 (6) of the Rules of Court 2012 had passed. Genting’s motion for leave to appeal to the Federal Court was also dismissed.

Nevertheless, while the ruling by the High Court was overturned, this case has made it clear that the courts will not be shy in limiting the powers of statutory bodies in cases where the collection and processing of personal data is found to be excessive. In the event that another similar application for judicial review surfaces, the decisions of the High Court, while not binding, may serve as an indication of how the courts may decide such cases in the future.

Ranjan Paramalingam & Anor v Persatuan Penduduk Taman Bangsar Kuala Lumpur

In the case of *Ranjan Paramalingam & Anor v Persatuan Penduduk Taman Bangsar Kuala Lumpur* [2023] 1 MLJ 459, the appellants alleged that, among other things, the residents’ association unlawfully obtained and misused the personal data of Bangsar Park residents under the guise of implementing a guarded neighbourhood security scheme. They claimed this amounted to a breach of the PDPA and sought an inquiry into the acquisition and use of their data, along with damages. In its decision, the High Court found that personal information was collected solely for security purposes with no evidence of misuse. As such, the High Court ruled that there was no breach of the PDPA.

Following the High Court's decision, the appellants decided to take the matter to the Court of Appeal. However, the appeal was subsequently dismissed. In reaching its decision, the Court of Appeal emphasised that, given the penal consequences arising from non-compliance with the PDPA, allegations of offences under the PDPA must be pursued strictly through the complaints mechanism provided by the JPDP. The Court of Appeal emphasised that, pursuant to Section 104 of the PDPA, complainants are required to submit a written complaint to the Commissioner, who is empowered to investigate and take appropriate action. Additionally, the Court of Appeal clarified that non-compliance with the PDPA cannot be used as a cause of action in a civil suit.

It is clear from this case that the primary mechanism available to any party aggrieved by another party's non-compliance with the PDPA lies with the complaint mechanism provided by the JPDP. Any party that attempts to pursue a civil claim for non-compliance with the PDPA will fail in their claim due to the fact that the PDPA does not provide for any means to make civil claims, unless and until a further decision of an appellate court in Malaysia determines otherwise.

2.3 Collective Redress Mechanisms

The PDPA does not provide aggrieved parties with the ability to pursue civil claims in the court, therefore collective redress is unlikely to succeed in Malaysia at this juncture (based on case law). Any complaints relating to a breach of the PDPA may only be channelled to the JPDP who may then carry out an investigation.

As such, there is currently no available collective redress mechanism available to the public to take action against any party in breach of the PDPA.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation Public Sector Agencies

The largest legislation pertaining to the sharing of data (both personal data and non-personal) between public sector agencies is the DSA, which has been approved

by the parliament of Malaysia but has yet to come into force. The DSA will establish the National Data Sharing Committee (NDSC) and sets down the general rules pertaining to the sharing of data between public sector agencies. This includes the methods to request data sharing, the purposes for which data may be shared, as well as the circumstances in which a public sector agency may deny a data-sharing request.

Additionally, the DSA imposes duties and obligations in relation to the protection of data that has been shared, such as the requirement to take necessary measures to ensure the security and privacy of data, including the protection of data from any loss, misuse, unauthorised or accidental modification, access or disclosure, alteration or destruction.

This obligation is similar to that provided under the PDPA in relation to the protection of personal data. Additionally, the obligation to protect data shared under the DSA extends to the recipient of the data as well as third parties who have been engaged by the data provider or recipient to conduct any data migration, data integration or data analytics work using the data shared under the DSA.

Finally, Section 23 of the DSA provides a general obligation of secrecy, imposing a requirement on any officer or servant of public sector agencies not to disclose any information obtained by them during the course of their duties.

Sector-Specific Requirements

Certain sectors in Malaysia impose additional requirements on the sharing of data through their regulations and guidelines.

For example, in the financial sector, Section 133 of the FSA prohibits the disclosure of any document or information relating to the affairs or account of any customer of the financial institutions, unless one of the conditions provided under Section 134 of the FSA is met. This applies to all documents or information relating to the affairs or account of the customer regardless of whether it is personal data or non-personal data.

The above requirements are further supplemented by various guidelines issued by the regulator, BNM. For example, the MCIPD lays out the specific conditions for permitted disclosures as well as the financial institution's obligations in relation to the protection of customer information, and notification requirements in the event of a breach.

Note that when processing personal data, financial institutions need to comply with the requirements under both the PDPA and FSA.

On the other hand, the disclosure of data under certain sectors is regulated under different acts. For example, the disclosure of credit information by credit reporting agencies is regulated by the Credit Reporting Agencies Act 2010 (CRAA). Any information subject to regulation by the CRAA is expressly excluded from the PDPA's scope. As such, when processing and disclosing credit information for the purpose of the credit reporting agency's business, the credit reporting agency is not required to comply with the PDPA and will instead be subject to the relevant requirements under the CRAA.

National Cloud Computing Policy

The National Cloud Computing Policy (NCCP) serves as a framework for cloud adoption across Malaysia's public, private and citizen sectors. In particular, it serves as a mandate for cloud adoption within government agencies.

While the NCCP merely sets out a framework for the adoption of cloud policy, it provides important insight into the likely direction the government wishes to take in relation to data sharing using cloud technology. Examples of this include Pillar One of the NCCP, which aims to prepare a cloud-based data integration platform for government agencies, allowing them to share data across agencies efficiently.

Nevertheless, the NCCP does not set out unique rules for sharing data across the cloud – rather, it references existing laws in Malaysia such as the PDPA and requires all stakeholders to adhere to the standards set under the PDPA. In cases where there is cross-border data transfer, the NCCP reminds all stakeholders that they may also be subject to the other nation's

personal data protection laws, such as the EU General Data Protection Regulation.

3.2 Interaction of Data Regulation and Data Protection

Public Sector Agencies

With regards to IP protection, Section 4 (2) of the DSA provides that any data shared under the DSA is deemed to be compiled pursuant to the relevant provisions of the statutes listed under the schedule of the DSA. This list includes Section 52 of the Copyright Act 1987 (the "Copyright Act") which regulates the disclosure of information obtained pursuant to the Copyright Act.

Therefore, any data that is considered to be the intellectual property of another person may only be shared in compliance with Section 52 of the Copyright Act.

Sector-Specific Requirements

In cases where the PDPA applies to the processing and disclosure of data, data controllers within these industries (such as the financial industry) are expected to comply with both the requirements under the PDPA as well as the relevant requirements under the applicable act, regulation or guideline. As such, financial institutions are required to comply with both the PDPA and secrecy obligations under the FSA and applicable guidelines. In cases where there are differing standards, the financial institution will be expected to comply with the stricter standard.

On the other hand, credit information subject to the requirements under the CRAA are expressly excluded under the PDPA. As such, credit reporting agencies are not required to comply with the PDPA when disclosing credit information. However, credit reporting agencies are still required to comply with the PDPA when dealing with non-credit information, such as the personal data of their employees.

In the case of IP protection of non-personal data, the Copyright Act will apply in all sectors, unless there is an act that expressly limits its application.

National Cloud Computing Policy

Part 4 of the NCCP (governance and oversight) sets down the applicable regulatory framework to ensure

compliance with data protection laws. In this respect, the NCCP requires all stakeholders to comply with the PDPA and international data protection laws. Additionally, cloud service providers are expected to implement certain general data protection measures, such as encryption, access control and audits.

3.3 Rights and Obligations Under Applicable Data Regulation

Apart from the rights and obligations provided under the PDPA, the previously mentioned laws do not provide for any additional rights and obligations as they are primarily focused on the disclosure obligations of the data controller, as opposed to providing rights to the data subjects.

3.4 Regulators and Enforcement Public Sector Agencies

Under Section 5 of the DSA, the NDSC was established, among other things, to oversee the implementation of the DSA, to take or recommend steps or administrative actions to resolve issues arising during the implementation of the act, and to formulate policies relating to databases for the purposes of data sharing under the DSA. The NDSC is comprised of representatives from several departments and ministries, including the secretary general of the Ministry of Digital, the chief government security officer and a representative of JPDP.

Additionally, Section 11 of the DSA provides the director general with several functions and powers, including the power to: implement policies and strategies related to data sharing, require any person to submit any relevant information or document for the purposes of performing the director general's duties, and to issue circulars or guidelines. Finally, Section 22 of the DSA gives police officers with the rank of sergeant and above the power to enforce, inspect and investigate any offence under the DSA.

That said, as the DSA has not yet come into force, there are currently no cases of enforcement arising under this act.

Sector-Specific Requirements

Data controllers in different sectors fall under different regulators. For example, BNM acts as the regulator

overseeing financial institutions and is responsible for issuing various guidelines, such as guidelines relating to the disclosure of customer information. Additionally, as the regulator, BNM has the power to investigate and impose penalties on financial institutions that fail to comply with the FSA or BNM's guidelines, including any failure to comply with the secrecy obligation under Section 133.

As a result of BNM's enforcement powers, in 2019 it issued two separate compounds and administrative monetary penalties. Similarly, several banks were taken to court for their or their employees' breach of Section 133 of the FSA.

Similarly, the Registrar of Credit Reporting Agencies is provided under Section 4 of the CRAA with the power to implement and enforce the CRAA, and is responsible for the monitoring, controlling, supervision and regulation of credit reporting agencies.

National Cloud Computing Policy

While the NCCP was overseen and developed by the Ministry of Digital in collaboration with several other ministries and government agencies (ie, the National Cyber Security Agency and the JPDP), the NCCP does not establish any enforcement agency or authority as it is merely a policy meant to guide and promote the adoption of cloud services.

4. Sectoral Topics

4.1 Use of Cookies

There are currently no rules governing online trafficking technologies such as cookies. As such, Malaysia does not impose any specific requirements relating to consent, opt-out models or cookie policies.

Nevertheless, while there are no strict requirements for the use of online tracking technologies, it is generally best practice for websites and other applications or devices to inform their users about the use of such technologies. Examples of such methods include simple pop-up notifications when a user first accesses a website or the insertion of a cookies policy in the website privacy notice or terms of use.

In cases where the online tracking technology processes personal data, the general requirements under the PDPA for the processing of personal data will apply. As such, any person who uses online tracking technology to process personal data will be required, among other things, to obtain consent for such processing, and to prepare and provide users with a privacy notice.

4.2 Personalised Advertising and Other Online Marketing Practices

Use of Personalised or Targeted Advertising

Personalised or targeted advertising refers to advertisements that are tailored to an individual's interest. In order to achieve this, personal data of that individual, such as their age, preferences, purchase history, web search history and nationality, will be collected and processed.

Therefore, any processing of personal data for the purposes of personalised or targeted advertising must be carried out in line with the PDPA. This includes the requirement to obtain the data subject's consent as well as providing them with a privacy notice which, among other things, informs them that their personal data will be used for the purposes of personalised or targeted advertising.

In the event that the personal data processed includes sensitive personal data, such as a person's physical or mental health condition, political opinions, religious beliefs, commission or alleged commission of an offence, or biometric data, the advertiser will be required to obtain the explicit consent of the data subject before it may carry out the processing of such data.

The above requirement to obtain consent extends to any personalised or targeted advertising directed at children. In the event that children's personal data is processed, the advertiser must first ensure that it has the consent of the parent, guardian or such other person who has parental responsibility over the child.

In addition to the general obligations under the PDPA, advertisers are also required, under Section 43 of the PDPA, to provide data subjects with the right to prevent the processing of their personal data for the

purposes of direct marketing. Therefore, any advertiser who uses personalised or targeted advertisements must ensure that they provide data subjects with options to prevent such processing. Examples of options that may be provided to data subjects include:

- providing them with an email address which may be used to contact the advertiser on personal data-related matters; or
- attaching a form on the website or app.

Finally, the commissioner of the JPDP intends to issue the ADMP Guideline, which seeks to regulate the processing of personal data through automated decision-making as well as profiling (which involves the processing of personal data to assess personal aspects of an individual, such as their personal preferences, interests and behaviour). Based on the Public Consultation Paper on the Guideline on Automated Decision Making and Profiling, the commissioner of the JPDP intends to provide data subjects with several rights, such as:

- the right to object or not be subjected to a decision based solely on automated decision-making;
- the right to information/transparency; and
- the right to request human review of any automated decision-making.

Therefore, any advertiser who relies on a fully automated system to profile and assess a data subject's preferences, interests or behaviour will be required to ensure that they comply with the requirements provided under the ADMP Guideline.

Delivery of Personalised or Targeted Advertisements

While there is currently no general prohibition against the means of delivering personalised or targeted advertisements, the Malaysian Communications and Multimedia Commission (MCMC) issued a Public Consultation Paper on Unsolicited Commercial Electronic Messages ("Unsolicited Messages PCP") in 2025 which, in line with Section 233A of the Communications and Multimedia Act 1998, intends to introduce a framework to address the issues of unsolicited commercial electronic messages.

The Unsolicited Messages PCP provides the following definitions:

- “unsolicited commercial electronic messages” – any commercial electronic message sent through any communication mode where there is no prior relationship between the sender and the recipient or no prior consent from the recipient;
- “commercial electronic message” – any electronic message sent by electronic means for the purpose of promoting, offering, marketing or supplying:
 - (a) products or services;
 - (b) land or any interest in land;
 - (c) business or investment opportunities; or
 - (d) a person or entity that provides such products, services or opportunities; and
- “electronic messages” – any message sent using a network service or applications service to an electronic address, endpoint, or similar communication mode.

Based on the Unsolicited Messages PCP, the MCMC is seeking to prohibit the following activities:

- the acquisition, distribution or usage of certain tools or software designed to extract electronic addresses from online sources or mechanisms that generate addresses through automated or pattern-based guessing (commonly known as “dictionary attacks”); and
- the sending of unsolicited messages to electronic addresses obtained from address harvesting (the automated collection of electronic addresses without consent) or dictionary attacks.

Therefore, in the event that the framework proposed under the Unsolicited Messages PCP is introduced by the MCMC, advertisers will be prohibited from sending any personalised or targeted advertisements via electronic message (such as an email) obtained from address harvesting or dictionary attacks. Nevertheless, the framework proposed under the Unsolicited Messages PCP is subject to change pending confirmation from the MCMC.

4.3 Employment Privacy Law Notification of Employees

Generally speaking, any processing of the personal data of job applicants and employees, whether it is for the purposes of adding them to the payroll, providing them with employment-related benefits or for employee disciplinary proceedings, is regulated under the PDPA. As such, employers must first provide the job applicants and employees with their privacy notice to inform them and obtain their consent for the processing of their personal data.

In cases where the employer wishes to process their personal data for new purposes not listed under the personal data protection notice, the employer will be required to obtain employees’ consent for the new purpose or amend the personal data protection notice and inform employees of the amendment.

The above-mentioned obligations also apply to the processing of personal data related to the monitoring of employees, use of the employer’s IT systems, bring-your-own-device policies and background checks. As there are no specific guidelines regulating the processing of personal data for the above-mentioned purposes, the standard obligations and requirements under the PDPA apply.

Regulations Relating to Third-Party Service Providers

Data processors

Additionally, employers often outsource many of their HR-related functions, such as the use of third-party service providers to administer payroll or to conduct background checks. As these third-party service providers process personal data on behalf of the employer for the employer’s purposes, the third-party service providers are considered to be data processors.

Under Section 9 (2) of the PDPA, data processors are required to provide the data controller (in this case, the employer) with sufficient guarantees in respect of the technical and organisational security measures governing the processing that is to be carried out on behalf of the employer, and take reasonable steps to comply with these measures. Item 14 of Paragraph 4.1 of the Personal Data Protection Standard further imposes a requirement on the employer to bind the

data processor with a contract. This is typically known as a data processing agreement, which includes the data processor's responsibilities as well as their obligations in relation to the protection of personal data and notification of data breaches.

Credit reporting agencies

In cases where employers wish to conduct background checks on a job applicant or employee through a credit reporting agency, the employers are generally required to first request that the job applicant or employee sign a consent form or letter authorising the disclosure of their information to the employer.

4.4 Data Protection in M&A

Apart from under the PDPA, there are no specific privacy requirements that specifically apply to M&A and asset deals. As such, when conducting any M&A transaction or asset deal, all parties to the transaction or deal are required to ensure that they have obtained the relevant consent, in line with the requirements under the PDPA.

Nevertheless, certain general privacy requirements that apply to entities that act within certain industries may apply in M&A transactions and asset deals. For example, Section 133 of the FSA imposes a general prohibition on disclosure by any financial institution and its employees concerning documents or information relating to the affairs or accounts of customers of such financial institutions, unless the disclosure meets the relevant conditions set out under Section 134 of the FSA.

Similarly, Section 153 of the Capital Markets and Services Act 2007 (CMSA) prohibits any member, employee or agent of the corporation from disclosing any information or document obtained in the course of their duties, except in the circumstances provided for under Section 154 of the CMSA.

In both cases, employees of the financial institution or corporation will be required to maintain secrecy and ensure that any disclosures made for the purposes of any M&A transaction or asset deal that they are involved in are made in line with the relevant legislation. Therefore, any party to M&A transactions or asset deals is reminded to ensure that they comply

with the PDPA as well as any other personal data or privacy-related obligation that may arise from relevant legislation, regulations or guidelines.

5. International Considerations

5.1 Restrictions on International Data Transfers

The primary act regulating the cross-border transfer of personal data is the PDPA. Section 129 of the PDPA provides that personal data may not be transferred outside Malaysia, except if one of the conditions under Sections 129 (2) or (3) is met. Examples of these conditions include:

- the data subject has provided their consent to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and data controller; and
- the data controller has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not be processed in the receiving place in any manner which would be in contravention of the PDPA.

Additionally, the Commissioner recently issued the Guideline on Cross Border Data Transfer (the "CBDT Guideline") which acts as a guide for compliance with the conditions under Section 129 (2) and (3) of the PDPA. For example, the CBDT Guideline provides that any person who wishes to rely on the consent of the data subject must first provide the data subject with a personal data protection notice containing the following details:

- the class of third parties to whom the data will be transferred; and
- the purpose of the transfer.

Therefore, any transfer of personal data outside Malaysia must be compliant with Section 129 of the PDPA, read in line with the CBDT Guideline.

ASEAN Framework on Personal Data Protection

As a member of the Association of South East Asian Nations, Malaysia is a signatory to the ASEAN Frame-

work on Personal Data Protection, which aims to harmonise data protection standards across South-East Asia. In line with the principles under the ASEAN Framework on Personal Data Protection, the ASEAN Model Contractual Clauses for Cross Border Data Flows (“ASEAN MCCs”) were introduced. The ASEAN MCCs sets out the responsibilities, security measures and obligations of parties to the ASEAN MCCs and are designed for the use of private-sector parties in ASEAN member states.

The use of the ASEAN MCCs was recognised in the CBDT Guideline as a method to comply with Section 129 (3)(f) of the PDPA, namely the requirement to take all reasonable precautions and exercise all due diligence. However, the CBDT Guideline recommends that data controllers review the ASEAN MCCs to determine whether any additional clauses need to be included.

In addition to the general personal data protection-related requirements, data controllers in certain sectors may also be required to meet the relevant sector-specific regulations or guidelines which impose requirements on cross-border data transfers. For example, financial institutions are required to comply with the relevant BNM guidelines, such as the RMiT, MCIPD and Outsourcing Policy Document. When engaging overseas cloud service providers, for example, financial institutions are required to first conduct due diligence on the service provider.

5.2 Government Notifications and Approvals

Malaysia currently does not require any registrations, filings or approvals from authorities for international transfers of data.

5.3 Data Localisation Requirements

There are currently no strict data localisation or residency obligations in Malaysia. However, transfers of personal data outside Malaysia will need to comply with Section 129 of the PDPA.

5.4 Blocking Statutes

There are currently no blocking or foreign-judgment control rules restricting foreign discovery, sanctions compliance, or cross-border disclosures in Malaysia.

5.5 Recent Developments

Section 129 of the PDPA was amended by the Personal Data Protection (Amendment) Act 2024, which came into effect on 1 April 2025.

The Amendment Act removed the whitelist previously provided for under Section 129 (1) of the PDPA as well as Section 129 (3), which provided that personal data may be transferred outside Malaysia if the “transfer is necessary as being in the public interest in circumstances as determined by the Minister”.

Additionally, the Amendment Act introduced two new conditions, allowing data controllers to conduct their own assessments and transfer personal data outside Malaysia if:

- the receiving place has any law in force that is substantially similar to the PDPA; or
- the receiving place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA.

The Commissioner has also issued the CBDT Guideline which is meant to be read together with Section 129 of the PDPA.

Trends and Developments

Contributed by:

Deepak Pillai, Yong Shih Han and Matthew Chang Jun Xiang
Christopher & Lee Ong

Christopher & Lee Ong (CLO) is located in Kuala Lumpur where it has a 25-practitioner strong TMT practice – the largest in Malaysia – which leads the Malaysian TMT legal landscape in terms of the range, breadth and depth of the legal services offered to clients. CLO advises major multinational corporations and conglomerates across banking, insurance, technology and telecommunications, and has done so for several decades. The firm also handles fintech, e-commerce, e-health and electric vehicles matters, as well as on-

line media and content. The firm has seen a steady increase in data centre and AI-related work, advising foreign operators establishing data centres in Malaysia and the ASEAN region, often alongside telecoms, corporate and tax considerations. CLO also regularly acts for global software giants that actively engage the firm as part of the Rajah & Tann Asia Network. In addition, the firm receives frequent instructions from European clients on Malaysian law in the context of GDPR compliance and cross-border data transfers.

Authors



Deepak Pillai heads CLO's TMT and data protection practice group and has practised in technology, telecommunications and data protection law since 1997. He advises international, private and public

sector clients on IT and cloud contracts, electronic commerce, online financial services, outsourcing, telecoms, cybersecurity, data protection, AI and online content, including in complex regulatory, policy and legislative matters. Deepak has been consistently recognised by leading legal directories since 2001, and is ranked in Band 1 for TMT in the Chambers Asia-Pacific Guide 2026. He also serves on the PDPA Appeals Tribunal and the Malaysian Bar's PDPA Committee.



Matthew Chang Jun Xiang is an associate in the technology, media and telecommunications and data protection and privacy practice group of CLO. He regularly assists with technology-related contracts,

including contracts relating to the implementation of IT systems, software development and subscription, maintenance and support, as well as service levels. Matthew also advises on data protection and cybersecurity clauses within IT contracts, including for clients operating within regulated sectors.



Yong Shih Han is a partner in CLO's technology, media and telecommunications and data protection practice group. She has been recognised by legal directories as an up-and-coming figure in TMT.

She regularly advises clients on a wide range of matters relating to information and communications technology, information security and data protection, telecommunications, and media and advertising laws. Her work includes drafting and advising on technology-related contracts and policies, regulatory and compliance matters, and issues that may lead to dispute resolution.

Christopher & Lee Ong

Level 22 Axiata Tower
No 9 Jalan Stesen Sentral 5
Kuala Lumpur Sentral
50470 Kuala Lumpur
Malaysia

Tel: +603 2273 1919
Fax: +603 2273 8310
Email: clo-info@christopherleeong.com
Web: www.christopherleeong.com

**Christopher
& Lee Ong**
Malaysia

The Personal Data Protection (Amendment) Act 2024 (the “Amendment Act”) was passed by the Malaysian parliament in Q4 of 2024, and introduced the first set of amendments to the Personal Data Protection Act 2010 (PDPA) since its inception. The amendments were introduced to deal with rapid advances in technology and the increasing use of personal data, while also bringing the PDPA in line with international personal data protection standards, such as the European Union’s General Data Protection Regulation (EU GDPR).

In addition to the amendments introduced by the Amendment Act, the Personal Data Protection Commissioner (the “Commissioner”) issued several guidelines to supplement the PDPA and to provide further guidance and clarification on the amendments introduced by the Amendment Act.

That said, Malaysia’s personal data protection framework is currently still being reviewed and further developments in 2026 are likely. These include amendments to the PDPA’s subsidiary regulation, the Personal Data Protection Regulations 2013 (“PDP Regulations”), as well as the issuance of several new guidelines.

This article highlights the key amendments introduced by the Amendment Act as well as the guidelines that have been issued by the Commissioner. It will also analyse the significance of the amendments and guidelines and their impact on data controllers and data processors. Finally, this article will highlight the upcoming amendments and guidelines, to provide

organisations with an indication of what they need to do in order to prepare for PDPA compliance in the future.

Key Changes

Replacement of the term “Data User” with “Data Controller”

The Amendment Act replaced the term “Data User” with “Data Controller”.

While this amendment was primarily cosmetic in nature, it helped align terminology used in the PDPA with that of other countries. Malaysian data controllers should therefore update their personal data protection documents and policies to reflect this change in terminology.

Recognition of biometric data as a type of sensitive personal data

The Amendment Act introduced “biometric data” as a new category of sensitive personal data. Sensitive personal data in turn is a subcategory of personal data that, due to its sensitive nature, is subject to stricter processing requirements. Examples of sensitive personal data include a data subject’s physical or mental health or condition, political opinions, commission or alleged commission of an offence, and more recently, biometric data.

Under the PDPA, the explicit consent of the data subject is required for the processing of their sensitive personal data (as opposed to consent for other types of personal data). Additionally, data controllers

are also expected to implement heightened security measures to protect sensitive personal data, as Section 9 of the PDPA provides that the security measures implemented must be commensurate with the nature of the personal data and the risk of harm involved.

While the Commissioner has not released any guidance or clarification as to what is considered to be biometric data, it is generally understood that biometric data will include the processing of fingerprint data, facial recognition, iris scans, signature identification, as well as behavioural data such as keystroke dynamics.

As a result of this amendment, data controllers that process biometric data will be subject to the additional requirements relevant for any processing of sensitive personal data and will be required to amend their internal data protection framework to ensure that these requirements are met.

Extension of the requirement to comply with the Security Principle to data processors

Prior to the Amendment Act, Section 9 of the PDPA (the “Security Principle”) only applied to data controllers. As a result of this, the obligations imposed on data processors, along with the legal ramifications for breaching these obligations arose purely from contractual arrangements with data controllers.

The amendment to Section 9 of the PDPA aims to bridge that gap by imposing a direct obligation on data processors to comply with the Security Principle. As a result of this, data processors are now independently responsible for implementing the appropriate security measures to protect personal data, including but not limited to implementing the minimum security standards (the “Security Standard”) as prescribed under the Personal Data Protection Standard 2015 (the “PDP Standard”).

Therefore, data processors will now be held directly liable for any breach of the Security Principle and will need to conduct assessments to ensure that their internal data protection frameworks are compliant with the Security Principle and Security Standard. Data controllers may also wish to review their data processing agreements and consider including new

clauses to reflect this new obligation on data processors.

Introduction of the requirement to appoint a data protection officer (DPO)

The Amendment Act introduced a new mandatory data protection officer (DPO) appointment obligation for data controllers and processors. This obligation is not a blanket requirement across organisations, as only data controllers and processors that meet the threshold provided under the Guideline on the Appointment of Data Protection Officer (the “DPO Guideline”) will be required to appoint a DPO, namely where the processing of personal data by the data controller or data processor involves:

- personal data of more than 20,000 data subjects;
- sensitive personal data (including financial information data) of more than 10,000 data subjects; or
- activities that require regular and systematic monitoring of personal data.

For the purposes of clarity, the DPO Guideline has provided several examples of what is considered to be “regular and systematic monitoring” of personal data, including:

- any activity where data subjects are tracked and profiled for purposes of behavioural advertising;
- the use of algorithms to monitor the searches and purchases of customers to offer recommendations based on these algorithms; and
- monitoring the wellness, fitness and health data of data subjects through wearable devices.

The DPO Guideline also sets out other requirements, such as the method of appointing the DPO, notification to the Commissioner of the appointment as well as the responsibilities of the DPO.

In addition to the DPO Guideline, the Commissioner has also issued further guidelines to address matters relating to the competencies, training and certification of DPOs, including the:

- DPO Competency Guideline;
- Management of DPO Training Service Providers Guideline; and

- DPO Professional Development Pathway & Training Roadmap.

As a result of these amendments, data controllers/processors will need to determine whether they are required to appoint a DPO and amend their internal policies and organisational structure to include this new role. Data controllers/processors that meet the threshold will be required to:

- appoint a DPO, whether internally or externally (ie, through a service provider, such as a law firm, that offers external DPO services);
- amend internal documents and policies to reflect the establishment of the DPO position in line with the responsibilities outlined under the DPO Guideline; and
- notify the Commissioner of the appointment.

Introduction of the mandatory Data Breach Notification regime

The Amendment Act introduced a new mandatory obligation on data controllers to notify the Commissioner and affected data subjects as to the occurrence of a personal data breach. This obligation is not a blanket requirement. Based on the Guideline on Data Breach Notification (the “DBN Guideline”), only data breaches that are of “significant harm” or “significant scale” are required to be reported to the Commissioner; whereas data breaches that are of “significant harm” require the affected data subjects to be notified.

For clarity, the DBN Guideline provides that a data breach is considered to cause or is likely to cause “significant harm” if there is a risk that the compromised personal data:

- may result in physical harm, financial loss, a negative effect on credit records, or damage to or loss of property;
- may be misused for illegal purposes;
- consists of sensitive personal data; or
- consists of personal data and other personal information which, when combined, could potentially enable identity fraud.

On the other hand, a personal data breach is of “significant scale” if the number of affected data subjects is more than 1,000.

Data controllers that hit the above-mentioned thresholds will be required to notify the Commissioner within 72 hours from the occurrence of the personal data breach. On the other hand, notification to affected data subjects must be completed no later than seven days after the initial data breach notification is made to the Commissioner.

In addition to the threshold and timelines, the DBN Guideline also imposes other requirements such as the information that is to be included in the notification, record-keeping requirements and containment actions that are to be carried out in the event of a data breach.

As a result of the amendments, data controllers will need to review their internal data protection framework to ensure that their data breach response plans (including notification to the Commissioner), as well as their records, are up to the standards required under the DBN Guideline.

Introduction of the new right to data portability

The Amendment Act has introduced a new right to data portability, which enables data subjects to request that a data controller transmit their personal data to another data controller, subject to technical feasibility and compatibility of format.

Based on the Public Consultation Paper on the Guideline on Data Portability (the “Data Portability PCP”), the specific guidance on the implementation of this right, including the types of personal data covered under this right, the mechanisms for transfer as well as the timelines for compliance with this right, will likely be covered under the upcoming guideline as and when it is issued.

Therefore, data controllers will need to wait for the issuance of the guideline to determine the policies and systems that may need to be put in place to provide this right to data subjects.

Amendment to the cross-border data transfer mechanism

The transfer of personal data outside Malaysia is generally prohibited, unless any of the conditions provided under Section 129 are met.

The Amendment Act has removed two conditions for the transfer of personal data, namely:

- The whitelisting/adequacy mechanism – under Sections 129 (1) and (2), data controllers were permitted to transfer personal data to countries on the “whitelist” of countries as determined by the Minister. The Amendment Act has removed this mechanism by deleting Section 129 (1) and amending Section 129 (2).
- Where the transfer is necessary as being in the public interest in circumstances as determined by the Minister (Section 129 (3)(h)). The Amendment Act has removed this by deleting Section 129 (3)(h).

Nevertheless, data controllers are not materially impacted by this as neither of the conditions was utilised, since no countries were placed on the “whitelist” and no circumstances were determined by the minister as being in the public interest.

Additionally, the Amendment Act amended Section 129 (2) to introduce two new conditions, namely if:

- the receiving country has laws in force that are substantially similar to those in Malaysia; and
- the receiving country ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA.

While the above two additions appear similar to the EU GDPR’s adequacy mechanism, they differ from the EU GDPR in that, while adequacy decisions in the EU are made by the regulators/authorities (ie, the European Commission), individual data controllers are given the power to make such assessments and decisions under the PDPA.

Additionally, the Commissioner has also issued the Guideline on Cross Border Data Transfer (the “CBDT Guideline”) which lays out the requirements for com-

pliance with each condition. For example, data controllers that wish to make use of the new conditions under Section 129 (2) will be required to carry out a transfer impact assessment. The CBDT Guideline also imposes certain requirements in general application, including the requirement to keep records of any cross-border data transfer.

The introduction of the CBDT Guideline therefore means that data controllers will be required to review their internal data protection framework to ensure that they meet the relevant requirements as provided under the CBDT Guideline.

Upcoming Changes to the Personal Data Protection Framework

As noted above, there are several upcoming amendments to existing regulations as well as new guidelines that are set to be issued. This section provides a brief overview of each amendment/guideline based on the public consultation papers that have been made publicly available. That said, any information provided here may still be subject to change by the Commissioner.

Amendment to the PDP Regulations

The Commissioner intends to amend the PDP Regulations to bring them in line with international standards and has previously issued a public consultation paper on the amendments to the PDP Regulations.

Based on this public consultation paper, several key definitions will be amended in or introduced to the PDP Regulations, including:

- the amendment of several key definitions for greater clarity (ie, “standard” will be amended to emphasise that any standards issued by the Commissioner constitute binding rules);
- clarification on the definition of consent;
- a new requirement to display the business contact information of the appointed DPO; and
- streamlining and strengthening the inspection powers of the Commissioner.

The amendments to the PDP Regulations are likely to be substantial and will require amendments to existing internal data protection frameworks. For example, in

the event that the amended PDP Regulations include stricter procedures and requirements for consent, data controllers may need to amend their internal data protection frameworks to update the way they obtain consent and (where necessary) obtain fresh consent from data subjects whose consent was collected prior to the introduction of the new procedures and requirements.

Amendment to the PDP Standard

The PDP Standard was issued in December 2015 to set out the minimum compliance standards and requirements in relation to the security, retention and data integrity principles under the PDPA (collectively, “Standards”).

In order to ensure that each Standard is brought up to date and in line with international best practices, the Commissioner intends to issue a revised PDP Standard. Based on the public consultation paper on the amendments to the PDP Standard, each Standard will be amended to introduce expanded measures to ensure that current operational risks are addressed (such as further measures related to the use of cloud computing services).

Additionally, in order to deal with the ever-evolving nature of data protection, the Commissioner has also proposed to shift the prescriptive approach of the PDP Standard to an outcome-based approach. By doing so, data controllers may employ various measures to ensure that the outcomes listed in the PDP Standard are met.

Due to the substantial number of amendments that have been proposed, data controllers (and data processors in relation to the Security Standard) will likely need to update their internal data protection framework to ensure that it is in line with the revised PDP Standard. Additionally, the outcome-based nature of the proposed revisions will mean that data controllers must regularly review and revise their internal policies and processes to ensure that the measures that have been implemented to meet each outcome are still relevant, up to date and sufficient, based on technological advances and their own personal data processing capabilities.

Introduction of the Data Portability Guidelines

As noted above, the Commissioner intends to introduce the Data Portability Guidelines to act as a guideline on the operation of the new right to data portability, and aims to provide data controllers with information such as the timeline to comply with requests, and the fees and methods for transmission of personal data pursuant to a data portability request.

Additionally, based on the Public Consultation Paper on the Data Portability Guideline, the Commissioner does not intend to require all data controllers to adopt or maintain new systems or processes for the purpose of complying with a data portability request. As such, data controllers will only be required to comply with the request if it is technically feasible to transfer a data subject’s personal data between the respective systems of the data controller and the receiving data controller.

Finally, the types of personal data subject to the right to data portability will likely be limited. Based on the current proposal, only personal data that is directly provided by the data subject and was provided based on consent or a contract to which the data subject is a party will be subject to this new right. Data controllers will not be required to transmit personal data classified as “inferred data” or “derived data”.

That said, data controllers will need to wait for the issuance of the Data Portability Guidelines to determine the extent of the changes to existing policies and systems required for compliance with the new right to data portability.

Introduction of the Guideline on Data Protection Impact Assessment (the “DPIA Guideline”)

The Commissioner intends to issue the DPIA Guideline which will in certain cases require data controllers to conduct mandatory data protection impact assessments (DPIAs) to determine whether the processing of personal data is likely to result in a high risk to the privacy of the personal data of data subjects.

Based on the public consultation paper for the DPIA Guideline, the Commissioner has proposed that data controllers conduct a DPIA if the quantitative threshold or qualitative thresholds as prescribed under the DPIA

Guideline have been met. In addition to the threshold for conducting a DPIA, the DPIA Guideline will set out the methods to conduct a DPIA, the requirements as to notification to the Commissioner, as well as any further obligations upon the conclusion of the DPIA.

Therefore, data controllers may wish to factor in the time and resources required to conduct a DPIA when planning any large-scale data processing projects, as the requirement to conduct a DPIA may result in delays in the commencement of the project. Data controllers may also wish to identify the personnel in the organisation with the capabilities to conduct a DPIA or (where permitted) identify external sources to assist with conducting any DPIA.

Introduction of the Guideline on Data Protection by Design (the “DPbD Guideline”)

The Commissioner intends to encourage data controllers in Malaysia to adopt the concept of Data Protection by Design (“DPbD”) in order to move from reactive to proactive data protection. As such, the Commissioner intends to introduce the DPbD Guideline, which aims to provide guidance on how to adopt and implement DPbD when complying with the personal data protection principles under the PDPA.

Based on the public consultation paper for the DPbD Guideline, the DPbD Guideline will set out the foundational principles of DPbD and guide organisations on the implementation of DPbD when complying with each of the PDP principles, including further guidance in relation to children’s privacy.

While the DPbD Guideline and the introduction of DPbD may improve the protection of personal data, data controllers will need to take a proactive stance in adopting DPbD, which may involve a significant revision of their respective internal data protection frameworks.

Introduction of the Guideline on Automated Decision Making and Profiling (the “ADMP Guideline”)

Owing to the rapid increase in the use of AI and machine-learning techniques to carry out automated

decision-making and profiling, the Commissioner intends to introduce the ADMP Guideline to provide guidance on the implementation requirements for the use of automated decision-making and profiling.

Based on the PCP for the ADMP Guideline, the Commissioner has proposed that the ADMP Guideline will only cover decisions which:

- are made by technological means without human involvement; and
- may legally or significantly affect an individual.

The above decisions will include the use of AI and Generative AI.

As such, any data controller which carries out any automated decision-making that achieves the above-mentioned threshold will be required to comply with the ADMP Guideline. This will include additional data subject rights and exceptions to those rights, and additional measures for the use of AI and Generative AI, and the processing of biometric data as well as the use of CCTVs.

Conclusion

The Amendment Act and issued guidelines represent a significant step forward in modernising Malaysia’s personal data protection framework and bringing it in line with international standards. Nevertheless, as the amended PDPA still retains distinct local nuances in both its scope and implementation, organisations that comply with alternative personal data protection frameworks (eg, the EU GDPR) are reminded not to assume automatic compliance, and to conduct a careful review of their respective personal data protection frameworks to determine compliance with the PDPA.

With the expected amendments to the PDP Regulations and PDP Standard, and the issuance of further guidelines on the horizon, Malaysia’s personal data protection framework is expected to evolve further. Organisations need to remain proactive in monitoring these PDPA-related developments and regularly update their internal data protection frameworks in order to ensure continued compliance with the PDPA.

MEXICO



Law and Practice

Contributed by:

Luciano Pérez and Allan Pastor
Nader Hayaux & Goebel

Contents

1. Legal and Regulatory Framework p.311

- 1.1 Overview of Data and Privacy-Related Laws p.311
- 1.2 Rights and Obligations p.311
- 1.3 Special Categories of Personal Data p.313
- 1.4 Processing of Personal Data for Research and Development Purposes p.313
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.313
- 1.6 Data Breach Requirement p.313
- 1.7 Regulators p.314
- 1.8 Enforcement Proceedings and Fines p.314
- 1.9 Enforcement Trends p.315

2. Privacy Litigation p.315

- 2.1 Privacy Litigation Overview p.315
- 2.2 Recent Case Law p.316
- 2.3 Collective Redress Mechanisms p.316

3. Requirements for the Protection and Processing of Non-Personal Data p.316

- 3.1 Objectives and Scope of Data Regulation p.316
- 3.2 Interaction of Data Regulation and Data Protection p.316
- 3.3 Rights and Obligations Under Applicable Data Regulation p.316
- 3.4 Regulators and Enforcement p.316

4. Sectoral Topics p.316

- 4.1 Use of Cookies p.316
- 4.2 Personalised Advertising and Other Online Marketing Practices p.316
- 4.3 Employment Privacy Law p.317
- 4.4 Data Protection in M&A p.317

5. International Considerations p.318

- 5.1 Restrictions on International Data Transfers p.318
- 5.2 Government Notifications and Approvals p.318
- 5.3 Data Localisation Requirements p.318
- 5.4 Blocking Statutes p.318
- 5.5 Recent Developments p.318

Nader Hayaux & Goebel is a leading full-service Mexican law firm with 22 partners and more than 40 associates. Its Data Privacy & Cybersecurity practice is led by one partner and supported by two associates, advising Mexican and foreign companies, both regulated and non-regulated, on compliance with Mexican data protection regulations and financial secrecy requirements. Based in Mexico City and supported by the firm's London office, the team stands out for its extensive experience in international and cross-border data privacy and cybersecurity matters, including the implementation in Mexico of foreign

regulations such as the GDPR. The practice provides comprehensive advice on privacy compliance, risk prevention and management, data breach response, biometric data processing and training programmes. Recent work includes advising a global videogame company on GDPR implementation, assisting international insurance companies with privacy notices and integrated compliance strategies, supporting a major e-commerce company on biometric data compliance, and conducting data privacy and financial secrecy audits for an insurance broker of a large automotive group.

Authors



Luciano Pérez is a partner at Nader, Hayaux & Goebel with more than 25 years of experience and is a core member of the firm's Corporate/M&A, Banking & Finance and Compliance practices, with a strong focus on data

protection and regulatory matters. His expertise includes data privacy and cybersecurity compliance, financial secrecy, regulated M&A and regulatory frameworks applicable to insurance, reinsurance, fintech and insurtech companies. He regularly advises Mexican and international clients on the implementation of cross-border data protection strategies, including GDPR-related compliance in Mexico, drafting and implementation of privacy notices, intragroup data transfer agreements, and integrated compliance and risk management frameworks. Luciano also has significant experience advising regulated entities on governance and compliance matters and serves as independent board member and secretary for insurance companies. He obtained his law degree from Universidad Iberoamericana and an LL.M. from Erasmus University Rotterdam, and he previously worked as a foreign associate in the banking and finance practice of Mayer Brown in Chicago. He is an active member of AMEDESEF (Mexican Chapter of AIDA), ANADE and ICC Mexico.



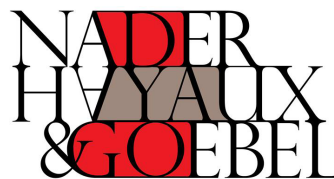
Allan Pastor is an associate at Nader, Hayaux & Goebel specialising in antitrust, compliance and data protection matters. He holds a law degree from Tecnológico de Monterrey and a diploma in Economic

Competition from Universidad Panamericana and the International Chamber of Commerce. His practice focuses on data protection compliance, regulatory risk management, and interactions with Mexican authorities. Allan has significant experience advising on data privacy compliance frameworks, including overseeing the internal data protection compliance system of one of Mexico's largest companies and representing matters before the national data protection authority. He has also been involved in merger notifications, investigations and formal proceedings before Mexico's antitrust authority. In addition, Allan regularly conducts internal compliance investigations for multinational companies, covering issues such as corruption, bribery, fraud and workplace misconduct, and participates in corporate compliance and regulatory audits, strengthening organisations' governance and risk management structures.

Nader, Hayaux & Goebel

Paseo de los Tamarindos
No. 400-B, Piso 7
Bosques de las Lomas
05120 CDMX
Mexico

Tel: +52 55 4170 3000
Email: info@nhg.com.mx
Web: nhg.mx



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

In Mexico, personal data protection is governed by a layered framework that applies nationwide to the private sector and, through a parallel regime, to the public sector. At its apex, the Political Constitution of the United Mexican States (*Constitución Política de los Estados Unidos Mexicanos*) recognises privacy and the protection of personal data as rights.

For the private sector, the main instrument is the Federal Law for the Protection of Personal Data Held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, or LFPDPPP). It governs the processing of personal data by private entities across Mexico and operates as a national baseline irrespective of the state in which an organisation is established or conducts its operations.

The LFPDPPP is supplemented by its Regulation (*Reglamento*), which develops and operationalises the statute and provides practical detail that the law sets out only at a high level. In addition, the private-sector regime is applied alongside secondary instruments issued by the competent authority – such as guidelines, criteria and recommendations – which shape interpretation and enforcement practice (together with the LFPDPPP and its Regulation, the “Private DPRs”).

Processing by the public sector is governed by a separate statutory regime, the General Law for the Protection of Personal Data Held by Obligated Parties

(*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), complemented by state-level legislation (together, the “Public DPRs”).

Mexican private-sector rules do not expressly claim extraterritorial reach. Cross-border scenarios are addressed instead through transfer and accountability mechanisms. Where a data controller transfers personal data to a third-party recipient that will act as an independent controller, the transferring controller must ensure that the recipient assumes and complies with obligations it is subject to under the Private DPRs.

Finally, the DPRs regulate personal data only (ie, information relating to an identifiable individual). Non-personal data will generally fall outside their scope, although the boundary is not clear-cut; certain processing may still be treated as personal data. Against that backdrop, as organisations adopt automated tools and AI-enabled processing, the Private DPRs remain the central reference point for lawful processing and accountability, while other legal regimes may impose parallel obligations.

1.2 Rights and Obligations

Principles and Requirements for Processing

The Private DPRs are built around a set of principles that must be observed cumulatively, as listed below. In practice, processing will be considered compliant only where these principles are embedded in the design and day-to-day operation of processing activities.

- *Lawfulness*: Processing must be grounded in a valid legal basis and carried out in accordance with the applicable framework.
- *Purpose*: Data may only be collected and used for specific and legitimate purposes.
- *Loyalty*: Processing must be carried out in a manner consistent with the individual's reasonable expectations.
- *Consent*: Processing requires the individual's consent, subject to recognised exceptions.
- *Quality*: Controllers should take reasonable steps to ensure data is accurate, complete and kept up to date.
- *Proportionality*: Only data that is adequate, relevant, and necessary for the stated purposes should be processed.
- *Information*: The individual must be informed about the details of the data processing.
- *Accountability*: Controllers must implement and be able to demonstrate compliance through governance measures, confidentiality duties, appropriate security controls, and effective oversight of processors and recipients.

Data Subject Rights and Remedies

Data subjects have a core set of rights that enable individuals to control and challenge the processing of their personal data ("ARCO Rights"), as listed below. In practice, data controllers should treat these rights as operational requirements, supported by clear request channels and internal procedures.

- *Access*: The right to confirm whether a controller processes the individual's data and, if so, to obtain access and information about the relevant processing.
- *Rectification*: The right to require correction or completion of personal data.
- *Cancellation*: The right to request deletion of personal data.
- *Opposition*: The right to object to processing in certain circumstances.
- *Revocation of consent*: The right to withdraw consent where it is the basis for processing.
- *Limitation of use or disclosure*: The right to request limits on certain uses or disclosures of personal data.
- *Complaint and redress*: Where the individual is not satisfied with the controller's response (or receives no response), the framework provides a route to seek review through the competent authority, which may issue binding determinations and trigger further oversight actions.

Main Compliance "To-Dos" for Companies

Though specific requirements for organisations vary depending on their business, operations and capabilities, the following workstreams are typically the core building blocks for adequate compliance:

- *Provide privacy notice*: Deliver a fully compliant privacy notice that includes, among other things, the purposes of data processing, the transfers to be carried out, the types of data to be collected, and the rights of the data subjects.
- *Obtain consent*: Collect and process personal data only after obtaining the data subject's consent (the type of consent will depend on the type of data to be processed).
- *Data quality*: Ensure that the personal data collected is accurate, relevant, and up to date for its intended purposes.
- *Data security*: Implement appropriate technical, physical and administrative measures to protect personal data from unauthorised access, loss or damage.
- *Guarantee ARCO Rights*: Allow data subjects to exercise their ARCO Rights and provide mechanisms and procedures that comply with the Private DPRs for their handling.
- *Retention period*: Store personal data only for the duration necessary to fulfil the purposes stated in the privacy notice.
- *Internal procedures*: Establish internal policies, procedures and training to ensure compliance with the Private DPRs, including appointing a Data Protection Officer or Department.
- *Data breach notification*: Notify data subjects in compliance with the requirements set forth in the Private DPRs in case the data controllers are subject to a data breach.
- *Third-party compliance*: Verify that any third-party data processor or recipient of personal data adheres to the Private DPRs and aligns with the controller's privacy notice.

1.3 Special Categories of Personal Data

Although the Private DPRs cover multiple categories of personal data, they single out sensitive personal data as particularly important to protect. Sensitive personal data is generally understood as personal data that affects an individual's most intimate sphere or that, if misused, could give rise to discrimination or entail a serious risk to the individual. Because of its heightened risk profile, sensitive personal data attracts stricter compliance expectations and a higher standard of care throughout the processing life-cycle.

In practical terms, controllers should ensure enhanced safeguards, including:

- *Stricter consent standard:* Processing sensitive personal data generally requires express, written consent.
- *Narrowly defined purposes and minimisation:* Purposes should be tightly framed and limited to what is genuinely necessary.
- *Clear outlines:* The privacy notice should clearly identify the sensitive categories of data involved and the relevant information about its processing.
- *Heightened security and confidentiality:* Controllers should implement stronger administrative, technical and physical measures.
- *Stronger vendor and transfer controls:* Where processors or third-party controllers are involved, contracts and transfer documentation should reflect the higher sensitivity.

For minors, the Private DPRs should be read alongside the overarching standard that the best interests of the child must be the primary consideration when designing and operating data processing, meaning a controller should prioritise a minor's welfare over commercial objectives.

In any event, data relating to minors – and, more broadly, data relating to any category of data subject – should be assessed against the applicable definition of personal data to determine the compliance requirements that follow, since such data may fall within that definition and therefore trigger the obligations set out in the Private DPRs.

1.4 Processing of Personal Data for Research and Development Purposes

Processing for research and development purposes is allowed if data controllers comply with the Private DPRs. Furthermore, the Private DPRs recognise the concept of dissociation (*disociación*), defined as a procedure through which personal data cannot be associated with the relevant data subject, nor can it be identified by virtue of its structure, content, or degree of disaggregation. Where dissociation is implemented with that effect, the resulting dataset would no longer qualify as personal data and may therefore be processed outside the scope of the Private DPRs. Any process that does not exclusively involve dissociated data remains subject to the Private DPRs.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

On automated decision-making, the Private DPRs take a more targeted approach than establishing an “AI risk taxonomy”. A data subject may oppose processing where (i) their personal data are used in automated processing that produces undesired legal effects or otherwise significantly affects their interests, rights or freedoms, and (ii) where the processing is intended to evaluate, analyse or predict aspects of the individual without meaningful human intervention.

Accordingly, specific and binding AI prohibitions are not features of the Private DPRs themselves; constraints arise from applying general rules. Specifically, a risk-sensitive compliance expectation is embedded through (i) heightened requirements for sensitive personal data, and (ii) security obligations that should scale with the risk profile of the processing (including foreseeable harm).

1.6 Data Breach Requirement

Under the Private DPRs, data controllers are expected to implement safeguards to protect personal data and to respond promptly where a security incident compromises it. Where a breach occurs, the Private DPRs require controllers to take the following steps:

- *Immediate containment and mitigation:* Take prompt measures to stop the incident and reduce exposure, including technical and organisational remediation.

- *Impact assessment*: Evaluate the main aspects of the incident and its legal implications for rights and obligations.
- *Notification to affected individuals where warranted*: Where the breach significantly affects data subjects' property or moral rights, the controller must notify the affected individuals so they can take protective steps. Notifications should be made without undue delay and in clear, accessible terms.
- *Post-incident assessment*: Determine and implement corrective actions and improvements to avoid future occurrences with the same characteristics.

1.7 Regulators

The 2024 constitutional reform provided for the dissolution of the National Institute for Transparency, Access to Information and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, or INAI) and the redistribution of its personal data protection mandates among various public bodies according to the type of entity being regulated. These changes took effect in 2025 upon the entry into force of new legislation.

For organisations, the most significant consequence is that the Ministry for Anti-Corruption and Good Government (*Secretaría de Anticorrupción y Buen Gobierno*, or SABG) now serves as the primary regulator of the private sector.

Furthermore, functions previously exercised by the INAI in the public sector were reassigned to diverse government entities, in some cases at the constitutional level. The National Electoral Institute (*Instituto Nacional Electoral*), for example, now oversees the processing of personal data by political parties.

From an enforcement perspective, matters under the Mexican data protection framework arise from data subject complaints, security incidents, or other events that put a processing practice in question; referrals or findings generated by the public sector; and ex officio initiatives in which the competent authority opens a file on its own motion. Co-ordination within Mexico is further shaped by the post-INAI allocation of mandates described above. Cross-border engagement is not organised around a “one-stop shop” model and

may instead be handled on a case-by-case basis when international elements are present (for example, cross-border transfers, foreign vendors or multinational group processing).

As mentioned in **1.1 Overview of Data and Privacy-Related Laws**, the guidelines, criteria and recommendations issued by the competent authorities typically operate as interpretative tools and enforcement benchmarks. Even where such guidance is not formally binding in the same manner as legislation, it often carries significant practical weight in audits, verification procedures and the authorities' assessment of compliance.

1.8 Enforcement Proceedings and Fines

Enforcement by the SABG is typically structured as a step-by-step administrative workflow. In practice, the first operational step for a data controller is usually receiving a formal request for information and documentation from the authority. The authority then reviews the response and may issue follow-up requests to address inconsistencies or obtain further evidence. Regardless, companies are subject to three main tracks: (i) the rights-protection procedure (focused on ARCO Rights disputes); (ii) the verification procedure (fact-finding and compliance review); and (iii) the sanctioning procedure (imposition of penalties). Although these tracks may be connected in practice, each follows its own sequence of procedural acts and statutory timeframes.

Decisions issued by the SABG may be challenged through judicial remedies. Specifically, affected parties may seek constitutional relief (*amparo*) against acts and resolutions of the SABG.

Rights-Protection Procedure

If the SABG receives and admits a rights-protection request from any data subject, the SABG serves it on the controller and requests a response with supporting evidence. The file then moves through an evidentiary phase, followed by final allegations, and ends with a binding decision. As a useful rule of thumb, the authority's decision is issued within 50 days, with the possibility of an extension for justified cause. Where the decision favours the data subject, the controller

is expected to implement the ordered measures and report compliance.

Conciliation may be promoted at any stage (subject to specific limitations). If the parties reach and comply with an agreement, the matter is generally closed without the need for a final decision on the merits.

Verification Procedure

Once verification is opened, the SABG typically begins with documentary information requests and may, where warranted, escalate to an on-site verification visit to confirm processing practices and controls. The overall verification stage is subject to a maximum duration of 180 days, with the possibility of an extension for justified cause.

Sanctioning Procedure

Sanctioning usually follows findings from a rights-protection or verification matter. It starts with formal service of the alleged infringement, after which the alleged infringer is given an opportunity to respond and submit evidence. The authority then closes the evidentiary record, receives final submissions and issues a final resolution. The sanctioning procedure has an overall statutory decision period of 50 days, with the possibility of an extension for justified cause.

Potential Sanctions and Remedies

Depending on the nature of the breach, exposure may arise on three tracks:

- *Administrative sanctions:* The SABG may issue orders (including warnings requiring corrective action) and impose fines, potentially multiple in a single matter. Where sensitive personal data is involved, the framework allows for fines to be doubled.
- *Criminal exposure:* Certain profit-driven conduct (eg, causing a breach for gains) may trigger criminal liability, with enhanced penalties where sensitive data is involved.
- *Civil liability (damages claims):* Affected individuals may pursue damages claims under general civil liability rules, with remedies centred on compensation rather than public sanctions.

1.9 Enforcement Trends

The SABG's recent communications and enforcement activity suggest the following:

- *Increased enforcement action:* A more assertive response to non-compliance, with investigations used as deterrence, and an explicit narrative linking breach cases to administrative fines and, in serious scenarios, criminal exposure.
- *Preventive engagement:* A parallel push for controllers to seek early institutional engagement and compliance support, signalling an emphasis on prevention alongside sanctions.
- *Execution and collection focus:* Increased attention to ensuring that sanctions are executed (including fine collection) and follow-ups on legacy matters previously treated as closed.
- *Reform-oriented posture:* An expressed intention to pursue updates to the federal and general data protection framework, suggesting enforcement may be accompanied by a legislative and policy push.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Privacy disputes in Mexico have not yet matured into a robust, standalone litigation stream. The legal system does not generally recognise a direct “private enforcement” action whose sole purpose is to vindicate data protection breaches in court. Rather, individuals who consider themselves affected typically need to frame their case as a civil liability claim, seeking damages for the harm allegedly caused by the relevant conduct.

This private route operates on a different logic from administrative oversight. Regulatory proceedings are designed to protect the public interest through corrective measures and sanctions (notably fines), whereas civil litigation is intended to compensate the claimant. Accordingly, the remedy most frequently pursued is monetary compensation. Assessment is usually case-specific and tied to the proof and seriousness of the alleged impact, rather than to a bespoke statutory tariff for privacy harm.

2.2 Recent Case Law

Unlike other jurisdictions, Mexico does not rely on case law to apply data privacy regulation. However, recent resolutions issued by Mexico's Supreme Court of Justice (*Suprema Corte de Justicia de la Nación*) have addressed modern issues, such as the role of search engines as intermediaries in internet access, their processing of personal data, and the implications for free speech rights.

2.3 Collective Redress Mechanisms

Mexican data protection law does not provide for collective administrative proceedings. Where a breach causes harm and civil liability arises, data subjects may pursue claims under the civil framework.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Non-personal data generally falls outside the scope of the Private and Public DPRs, which apply only to the processing of personal data. Information labelled “non-personal” may still be treated as personal data where individuals can reasonably be identified from the dataset itself or by linkage with other data. By contrast, data that has been robustly dissociated, such that identification is not possible, will typically remain outside the data protection regulations.

Mexico does not have a dedicated, cross-sector legal framework governing non-personal data access and sharing (including for IoT or cloud environments). Instead, non-personal data governance is primarily driven by general legal protections (notably confidentiality and trade secrets), sector-specific rules (such as financial secrecy and open finance for Mexican financial institutions), cybersecurity expectations, and contractual boundaries among data holders, service providers and data users.

3.2 Interaction of Data Regulation and Data Protection

Where a dataset includes both personal and non-personal elements, the approach is essentially cumulative: privacy rules govern the personal-data layer, while other legal regimes govern the non-personal

value layer (confidentiality, trade secrets and IP), with contracts typically co-ordinating how these obligations operate in practice.

Overall, the interaction is less about statutory “data access rights” and more about layering: the Private DPRs set the compliance perimeter for identifiable information; confidentiality and IP rules protect the commercial value of non-personal datasets, as well as contractual arrangements allocate rights, responsibilities and risk among data holders, service providers and data users.

3.3 Rights and Obligations Under Applicable Data Regulation

Unless a dataset has been properly dissociated so that individuals are no longer identifiable, the processing will generally fall within the scope of the data protection regime, and the primary rights available to individuals are the ARCO Rights.

3.4 Regulators and Enforcement

Under Mexico's current framework, non-personal data is not overseen by a single, cross-sector regulator; instead, the applicable rules and enforcement authorities vary depending on the nature of the dataset and the sector in which it is used.

4. Sectoral Topics

4.1 Use of Cookies

The Private DPRs require data controllers to inform data subjects when using remote or local electronic, optical or other technologies that automatically and simultaneously collect personal data upon interaction, such as cookies. This notification must be provided at the moment of contact through a visible communication or warning that details the use of such technologies, the data collected, and how to disable them.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised and targeted advertising under the Private DPRs is regulated in the same way as other data processing. A key aspect is the distinction between primary and secondary purposes: processing that is necessary to provide the product or service request-

ed by the individual will be categorised as primary, whereas advertising, commercial prospecting and similar activities will generally fall within secondary purposes (subject to a case-by-case assessment).

Where marketing or profiling is treated as a secondary purpose, the data controller must ensure that it is clearly disclosed in the privacy notice and that individuals are given straightforward mechanisms to withhold consent or withdraw consent for those purposes. Individuals may exercise the right of opposition to processing for secondary purposes, which is particularly relevant where profiling or behavioural targeting is involved.

Additional sensitivity arises in two scenarios. Firstly, it applies where marketing relies on sensitive personal data. Secondly, where advertising relates to minors, controllers should apply a heightened standard of care and avoid practices that could be seen as undermining a child's best interests, as discussed in **1.3 Special Categories of Personal Data**.

4.3 Employment Privacy Law

Mexican data protection rules apply to employers in the same way they apply to any other data controller. Accordingly, an employer that collects or uses employee or candidate information must comply with the Private DPRs throughout the employment lifecycle.

In practice, this means that workplace monitoring and the use of IT systems should be structured around necessity and proportionality. Although corporate devices and accounts are work tools, employees retain privacy interests, and monitoring should be limited.

4.4 Data Protection in M&A

In M&A transactions, the regular data privacy requirements apply. Personal data often becomes part of the due diligence exercise, the integration planning and – depending on the structure – the assets being acquired. Where that is the case, the parties should also treat data protection as a discrete workstream and implement controls designed to ensure compliance with the Private DPRs throughout the deal cycle.

In practice, companies should consider the following steps:

- Confirm whether personal data is in scope (and at what sensitivity).
 - (a) Identify whether the transaction involves personal data at all, and whether any sensitive personal data is implicated.
 - (b) Map the categories of data likely to be reviewed or transferred (eg, employee, customer, supplier, health, financial, geolocation).
 - (c) Confirm that the contemplated uses of the data (diligence, valuation, integration) align with the principles of purpose limitation and proportionality.
- Define how, when and by whom the data will be accessed.
 - (a) Determine where relevant datasets are stored and how they will be made available (eg, data room, clean teams, extracts, redacted samples).
 - (b) Identify the recipients (deal team, advisers, auditors, consultants, potential buyers) and apply need-to-know access controls.
 - (c) Clarify where the data will be held during the process and after closing, including any cross-border elements.
- Implement deal-specific safeguards and documentation.
 - (a) Put in place appropriate confidentiality and data-handling terms, including restrictions and covenants on processing, onward disclosure, retention and deletion/return.
 - (b) Where the buyer (or advisers) will process data on behalf of the seller, adopt suitable processor-type controls; where disclosure is to an independent recipient, ensure the transfer is properly documented and consistent with the applicable privacy notice and any required consents.
 - (c) Apply stricter controls where sensitive data is involved, including tighter access, segmentation and enhanced security measures.
- Assess security posture and breach history.
 - (a) Identify prior security incidents affecting relevant datasets and evaluate any open remediation items.
 - (b) Assess foreseeable breach risks at three points

- pre-closing, during diligence/transition and during post-closing integration – and align technical and organisational measures accordingly.
- Validate compliance foundations.
 - (a) Confirm that the data was collected and is being used under appropriate transparency practices (privacy notices) and, where required, valid consents.
 - (b) Review whether existing security measures are proportionate to the risks and adequate for the intended deal-related processing and subsequent integration.

This approach helps reduce unnecessary exposure during due diligence, supports smoother post-closing integration, and mitigates regulatory and litigation risk when personal data forms part of the transaction footprint.

5. International Considerations

5.1 Restrictions on International Data Transfers

The Private DPRs permit cross-border transfers of personal data, provided the transferring data controller complies with the applicable transparency and, where required, consent requirements. For these purposes, a transfer should be understood broadly as any communication, disclosure or making available of personal data to a third party other than the data subject (or its subsidiaries, affiliates and service providers), within or outside Mexico. Importantly, the fact that a transfer is international does not dilute the controller's obligations: the general processing requirements continue to apply, and cross-border transfers are treated as an extension of the originating processing activity rather than as a separate, unregulated step.

A defining feature of the Mexican approach is that the foreign recipient must assume obligations equivalent to those borne by the transferring controller under the Private DPRs. In practice, this is typically implemented through contractual arrangements. While the DPRs allow controllers to rely on a range of legal instruments to meet their duties, contractual clauses are the principal mechanism expressly contemplated for

international transfers. As a baseline, transfer clauses should ensure that:

- the recipient undertakes to comply with obligations equivalent to those applicable to the transferring controller under the Private DPRs; and
- the recipient agrees to process the data consistently with the scope of the authorisations and limitations communicated to the data subject through the applicable privacy notice (including the stated purposes and any transfer conditions).

Where there is uncertainty about whether a contemplated cross-border transfer aligns with the Private DPRs, a controller may seek a non-binding view from the competent authority on the transfer's permissibility and the adequacy of the proposed safeguards.

5.2 Government Notifications and Approvals

No government notifications or approvals are required to transfer data internationally. The data controller must include transfers of personal data in the privacy notice to inform the data subject when consent is required.

5.3 Data Localisation Requirements

Mexico's regulation on personal data protection (both Private and Public DPRs) does not establish specific data localisation requirements, nor do they contemplate the need to store personal data in-country. Therefore, under the scope of personal data protection, data can be transferred internationally; however, data controllers are still required to implement measures to safeguard data and comply with the requirements for transferring personal data established in the DPRs, such as providing a privacy notice to the data recipient.

5.4 Blocking Statutes

Aside from the nation's sovereignty and the provisions of the Constitution, there are no specific statutes regarding "blocking".

5.5 Recent Developments

As discussed in 1.7 **Regulators**, recent regulatory changes primarily focused on dissolving the INAI and reallocating its responsibilities. On this note, the Regulation of the LFPDPPP has not been amended

to properly address these changes; therefore, further updates are expected for this instrument. Additionally, while several legislative initiatives on specific data protection matters were proposed in 2025, none have been enacted; however, the SABG has stated that additional regulatory changes are needed.

Trends and Developments

Contributed by:

Daniel Villanueva Plasencia, Carlos Vela-Trevino and Paulina Bojalil Warth
Baker McKenzie

Baker McKenzie has 60 years of experience in Mexico and has a strong presence in five states of the country, namely Mexico City, Guadalajara, Juárez, Monterrey and Tijuana. As the most recommended law firm in major practice areas around the world, its offices are constantly involved in major mergers and

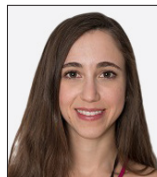
acquisitions and sophisticated financial transactions. The firm's global presence allows it to rapidly create teams of specialists in multiple jurisdictions to meet the needs of its clients. Baker McKenzie is known locally for the highly specialised and industry-focused knowledge of its attorneys.

Authors



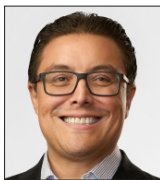
Daniel Villanueva Plasencia is a partner in the Intellectual Property practice group at Baker McKenzie Guadalajara. With over 15 years of experience, he specialises in data privacy, information security and

cybersecurity matters. His expertise extends to regulatory issues related to information technologies and consumer protection, as well as intellectual and industrial property – with a particular focus on digital environments, including the use and licensing of trade marks, patents and copyrights. His advisory services cover a broad spectrum including regulatory restrictions, intellectual property, data privacy and security. Daniel advises on global data privacy, data protection, cybersecurity, digital media, and legal and regulatory issues.



Paulina Bojalil Warth is an associate in the Mexico City office of Baker McKenzie with seven years of experience. She specialises in data privacy and security, technology, media and telecommunications (TMT),

as well as e-commerce, and commercial and software contracts. Additionally, she handles matters related to the aeronautical industry. Her primary areas of expertise include advising on technology, data privacy and security, telecommunications, e-commerce, consumer protection and general contractual law. Paulina has advised global companies both in Mexico and abroad. Her work spans across global data privacy and security strategies, cross-border deals, global contractual transactions, and assisting with market entry and service implementation.



Carlos Vela-Trevino is a partner in Baker McKenzie's Information Technology & Communications practice group in Mexico City, and the head of the firm's Technology, Media & Telecommunications (TMT) industry

group in Mexico. Carlos is recognised by Chambers as one of the country's leading TMT lawyers. He advises on corporate and commercial matters, including e-discovery, FCPA investigations, e-commerce, direct marketing, privacy in the workplace, litigation and M2M communications. Carlos is proficient in all key areas of IT/C law including telecoms regulation/licensing; software, cloud and technology contracts and procurement; design, implementation and monetisation of e-commerce portals; marketing, consumer protection and copyright.

Baker McKenzie

Pedregal 24, 12th floor
Lomas Virreyes / Col. Molino del Rey
México City, 11040
Mexico

Tel: +52 55 5279 2900
Email: Adrian.Rodriguez-Montfort@bakermckenzie.com
Web: www.bakermckenzie.com/en/locations/latin-america/mexico



Executive Summary

Mexico's privacy architecture was fundamentally reshaped in 2025. A sweeping constitutional reform dissolved the autonomous data protection regulator and ushered in a new statutory framework, including a revised Federal Law for the Protection of Personal Data Held by Private Parties ("LFPDPPP 2025", for its initials in Spanish), effective from 21 March 2025. Enforcement authority over the private sector moved to the Secretariat of Anti-Corruption and Good Governance (SABG, for its initials in Spanish), an executive-branch body, while judicial review now proceeds through specialised federal courts via amparo.

For businesses, the impact has been immediate: refreshed definitions, tighter consent and privacy notice mechanics, and a new enforcement and litigation pathway, all unfolding during a transitional period in which implementing regulations remain pending and further revisions to the LFPDPPP 2025 may result in a new law which it is rumoured will be issued in 2026. This analysis reflects the legal and regulatory position as of February 2026.

At the same time, Mexico is rolling out a biometric digital identity system (*CURP biométrica* and *Llave MX*), a National Cybersecurity Plan (2025–2030) and seeking real-time access to digital platforms transactional information, including personal data of taxpayers/users for tax audit purposes. Together, these initiatives elevate risks and compliance expectations regarding governance, security, identity proofing and electronic evidence preservation. Cross-border strategies should also anticipate the USMCA joint review in 2026 and Mexico's engagement with the UN Con-

vention against Cybercrime, both of which will influence data flow governance and incident response standards.

Treat 2026 as a year to reset the foundations: assess, harden and document privacy and security programmes now, allowing future regulatory updates to require only adjustments, rather than a full redesign.

1. Introduction

Mexico's data protection landscape has undergone a profound transformation during 2025–2026. Rather than incremental reform, change has been driven by institutional restructuring, political realignment, and an ambitious digital transformation agenda from the government. These dynamics have created a complex compliance environment in which companies must plan for uncertainty.

Although the market anticipated a substantive modernisation of Mexico's privacy framework, particularly around the European General Data Protection Regulation (GDPR), artificial intelligence (AI), automated processing and decision-making, and algorithmic transparency, the enacted private sector law largely preserves the architecture of the 2010 regime. As a result, organisations are increasingly relying on internal governance, risk-based analysis and international standards to bridge regulatory gaps while awaiting secondary legislation, new enforcement priorities from the new data protection authority and early judicial interpretation.

The reforms originate in a November 2024 constitutional amendment that eliminated seven autonomous

agencies, including the National Institute for Transparency, Access to Information and Personal Data Protection (INAI), which had served as Mexico's data protection authority. Such reform was effective in early 2025. Decrees published in the Official Gazette in March 2025 formalised a new law (LFPDPPP 2025) for the private sector and a General Law governing public sector processing of personal data, both effective from 21 March 2025.

As of early 2026, implementing regulations have not yet been published. SABG initiated stakeholder dialogues in January 2026, but no revised regulations or technical corrections have appeared in the Official Gazette. No judicial precedents from the specialised courts have been reported publicly. SABG has, however, signalled increased scrutiny following several high-profile cyber incidents during the end of 2025 and early 2026, suggesting that enforcement activity may resume before the regulatory framework is fully harmonised.

2. Legislative Shifts and Regulatory Redesign

2.1 The 2025 reset: new laws, new authority, new courts

On 20 March 2025, Mexico enacted a package of reforms realigning its data protection framework with the dissolution of INAI. Central to this package are the new LFPDPPP (private sector) and the General Law on the Protection of Personal Data Held by Obligated Subjects (public sector) (LFPDPPSO, for its initials in Spanish), both effective the following day.

Private sector oversight now resides with SABG, an executive-branch ministry. Appeals against enforcement decisions proceed through specialised federal courts via amparo. This institutional redesign matters in practice: enforcement culture, evidentiary expectations and timelines are likely to differ from those developed under INAI. During this bedding-in period, companies should document compliance judgments and risk-based decisions carefully, anticipating later scrutiny by courts rather than administrative precedent.

2.2 LFPDPPP 2025: continuity over transformation

The LFPDPPP 2025 preserves the core principles of the 2010 law: lawfulness, consent, information, quality, purpose, loyalty, proportionality and accountability.

However, critical definitions such as “data processing”, “personal data” and “data controller”, which were previously aligned with international frameworks such as the GDPR, have now been altered, creating interpretative risks. Privacy Notices must now describe processing activities with greater precision, disclose whether sensitive personal data is being processed, and distinguish those activities which the data subject may choose to opt-in to or opt-out from before the collection of data takes place.

Structurally, however, the statute remains familiar. The absence of a dedicated framework for AI governance, automated decision-making or algorithmic transparency is widely viewed as a missed opportunity. Until secondary regulation or future legislative amendments address these areas, organisations must rely on internal controls and risk assessments following a data protection impact assessment methodology, together with international benchmarks to manage exposure.

2.3 Key definitional and structural updates

Updated definitions emphasise the breadth of “personal data” and recalibrate consent standards towards specificity and revocability. Privacy notices must be clearer and more granular, identifying categories of data and linking them to defined purposes. These changes heighten supply-chain accountability and reinforce the need for auditable data-processing agreements.

2.4 Consent, notices, transfers and supply-chain accountability

Consent under the new statute must be free, specific and informed, with diminished tolerance for bundling multiple purposes under broad compatibility theories. When purposes change materially, fresh consent should be obtained. Privacy notices must distinguish which purposes require consent and clearly identify sensitive data.

Although the statute no longer mandates a standalone section relating to transfers in comprehensive notices, transfer obligations themselves remain intact. Organisations should design separate, standardised transfer workflows and obtain consent where required. The definition of publicly accessible sources has been nar-

rowed to those explicitly authorised by law, excluding datasets obtained through informal or unlawful means.

Administrative fines can reach up to 320,000 UMAs (approximately MXN40 million), with enhanced penalties for sensitive data and repeat violations. Appeals against SABG resolutions proceed through amparo, reinforcing the need for precise lawful-basis mapping, consent records and decision logs.

2.5 Implementing regulations and transitional risk

The legislative package contemplated harmonised regulations following enactment. In practice, most organisations continue to rely on the 2011 Regulations and legacy guidance, interpreting references to the former authority as applying to SABG.

As of February 2026, no updated regulations or technical corrections have been published. Market speculation persists that additional legislative amendments could precede finalised regulations, potentially rendering draft rules obsolete. In this environment, conservative compliance strategies are prudent: overdisclosure in notices, disciplined purpose limitation, low-friction re-consent mechanisms, and meticulous documentation of interpretative choices.

2.6 Institutional transition: from INAI to SABG

The shift from an autonomous regulator to an executive-branch authority marks a structural pivot. During this transition, enforcement activity slowed and official guidance became limited, prompting consumer protection agencies, financial regulators and other sector-specific authorities to step in and fill the gaps.

Given her record of strict oversight of tax regulation while serving at the tax authority, the new head of SABG was widely expected to take an equally firm approach to data protection enforcement. Her background suggested that SABG would not hesitate to pursue significant actions against major companies, including technology operators.

Early enforcement actions that occurred in January 2026 following several highly publicised cyber incidents affecting Mexican governmental and private organisations and data subjects already illustrate this shift, with authorities initiating formal proceed-

ings immediately and making them public from the outset. This represents a sharp departure from prior INAI practices, where preliminary review stages often allowed early clarification or resolution before escalation. The new approach indicates a greater willingness to pair legal processes with public communication to enhance deterrence. At the same time, growing calls for stronger sanctions indicate that enforcement will intensify as broader legislative reforms move forward.

While no public sanctions or judicial decisions have been issued as of early 2026, early probes suggest heightened scrutiny of data controllers and processors' conduct and incident handling. Companies should prepare for uneven enforcement criteria and prioritise defensible governance, DPIA-style analysis for high-risk processing (such as AI and biometrics), and investigation-ready documentation.

3. Cybersecurity: Strategy Ahead of Statute

Mexico still lacks a single comprehensive cybersecurity statute. Obligations remain distributed across criminal law, data protection rules and sectoral regulation. In late 2025, however, the federal government presented a National Cybersecurity Plan (2025–2030) and a General Cybersecurity Policy for the federal administration.

These instruments signal a more co-ordinated approach to cyber risk, including centralisation of CSIRTs/CERTs, phased adoption of AI-driven defences and enhanced co-operation on incident response. Mexico remains highly exposed to ransomware, with over 150 publicly reported victims since 2019. For companies, governance is the priority: integrate cyber risk into enterprise risk management, align incident response with electronic-evidence preservation, maintain 24/7 law-enforcement contact protocols and conduct regular tabletop exercises.

Sectoral alignment is emerging, particularly in financial services and critical infrastructure, where supervisory expectations already include breach reporting and resilience testing.

4. Mexico's New Identity Verification Framework: Key Implications for Companies

Mexico's emergency involving forced disappearances has prompted the government to introduce sweeping reforms, centred on the creation of a unified identity verification framework known as the *Plataforma Única de Identidad* (PUI). Designed to consolidate biometric and administrative records, the PUI enables faster cross-agency verification and seeks to strengthen national search and identification capabilities.

A key element of the new regime is the transition to the electronic, biometric CURP, a new national identity document which replaces legacy identifiers and incorporates facial images, fingerprints and digital signatures. Any organisation classified as a "Diverse Institution", that is, any entity maintaining records useful for identifying individuals, will be required to collect the electronic CURP. This broad definition encompasses companies with customers, users, or patient, student or employee databases across sectors such as finance, healthcare, telecommunications, insurance, transportation, education, private assistance and delivery services. Consequently, even businesses with no connection to public security must interconnect with the PUI and collaborate with law enforcement authorities, marking a significant compliance shift for nearly all data processing entities in Mexico.

To comply, organisations must connect to the PUI through secure web-service protocols, implement internal search capabilities (basic, historical and continuous), adopt cybersecurity measures aligned with a technical manual, expand breach-notification procedures and maintain updated compliance documentation. Sanctions for non-compliance are substantial, ranging from USD60,000 to USD120,000.

These reforms require companies to redesign onboarding processes to register the electronic CURP, align systems with the technical manual, strengthen privacy and cybersecurity controls, and reassess cross-border data transfers involving identity attributes. Ultimately, it is clear that Mexico is moving towards a model where identity governance and public-security objectives converge, demanding robust, multidisciplinary compliance strategies from all organisations operating in the country.

5. Real-Time Data Access Requirements: Mexico's New Article 30-B Framework

Article 30-B of Mexico's Federal Fiscal Code, effective from 1 April 2026, will require certain digital platforms to grant the tax authority (SAT) permanent, real-time access to transactions databases for tax-verification purposes. This represents a significant departure from traditional audit mechanisms, which operate through targeted, time-bound information requests. By enabling continuous visibility into operational and transactional data, the reform creates a potential risk of exfiltration of personal data relating to customers.

This real-time monitoring obligation raises considerable privacy and cybersecurity concerns. Granting SAT officials unrestricted system access increases the risk of data misuse, unauthorised extraction, or cross-referencing of sensitive information for purposes unrelated to tax compliance. To mitigate these risks, companies should deploy strict technical and procedural controls, such as compliant platforms, detailed access logs, and mandatory on-screen notices reminding officials of their legal duties and liabilities.

For digital businesses operating in Mexico, Article 30-B will require a comprehensive compliance strategy. Organisations must ensure that tax-verification access is tightly constrained, auditable, and compatible with their confidentiality obligations. This includes implementing protective controls, updating internal policies and reassessing how high-volume data environments are monitored. Ultimately, the proposal signals a shift towards far more intrusive digital-economy enforcement, and companies will need to balance tax compliance expectations with robust protections for user data and corporate systems.

6. International Context: USMCA and the UN Cybercrime Convention

The USMCA Digital Trade Chapter continues to anchor Mexico's cross-border data strategy. The first joint review, scheduled for July 2026, is expected by many observers to increase discussions regarding cybersecurity co-operation, AI governance and automated decision-making transparency. Even in the absence of immediate binding outcomes, supervisory expectations and contractual standards often evolve in parallel with these reviews.

Separately, the UN Convention against Cybercrime, opened for signature in Hanoi in October 2025, establishes a framework for harmonised cybercrime definitions, 24/7 co-operation mechanisms and standardised electronic-evidence preservation. Mexico has characterised the Convention as a historic step towards improved evidence sharing. Corporate incident response programmes should anticipate expedited evidence requests and stricter chain-of-custody expectations.

7. Practical Roadmap for Doing Business in Mexico in 2026

A practical compliance roadmap should begin by determining whether a company falls within the scope of a “Diverse Institution” under Article 12 Bis of the *Ley General en Materia de Desaparición Forzada de Personas*, as amended in 2025, and by extension under the interconnection obligations created through the *Ley General de Población*, as well as whether it qualifies as a “Digital Platform” under Article 30-B of the Federal Fiscal Code. This threshold assessment will determine the breadth of compliance duties and the pace at which implementation must occur.

Once within scope, organisations should begin by mapping the types of data they hold, focusing specifically on transaction-level information and identity-related data that may be subject to access requests. This includes both historical and recent information that may need to be made available to different authorities operating under varying technical environments and procedural rules. Any collaboration with authorities must also ensure robust traceability and auditable evidence of access.

In parallel, companies should assess the maturity of their cybersecurity position against OWASP and NIST benchmarks, as required by the PUI framework. This involves aligning internal programmes with national cybersecurity expectations, assigning accountable owners, inventorying critical assets, exercising incident response capabilities and integrating mechanisms for the preservation of electronic evidence. From there, organisations should initiate the development and deployment of the mandatory PUI endpoints, together with the redesign of onboarding and

data collection processes to ensure compliant intake and management of identification data.

These operational changes must be accompanied by a full refreshment of privacy notices. Notices should be concise, specific, and explicit about categories of personal and sensitive data. Any consent-dependent activities must be clearly identified, and cross-border transfers must be supported by standardised, well-documented workflows. Consent management itself requires renewed rigour, as legacy reliance on broad or “compatible” purposes is becoming increasingly unsustainable. If a company is using AI tools to monitor or predict employee conduct or behaviour, implementation should comply with privacy laws, and candidate and employee privacy notices should be refreshed as well.

Data processors must be treated as material compliance risks, with contracts that reflect statutory obligations concerning security, sub-processing controls, breach notification standards and audit rights.

Finally, companies should re-baseline their records of processing, lawful basis mapping and accountability documentation. With judicial oversight potentially weakening, investigation-ready files, such as DPIAs for high-risk processing, incident reports, vendor due diligence records, system logs and training documentation, are becoming essential safeguards. This strengthened governance will be critical as organisations navigate a regulatory environment in which identity, security and enforcement frameworks converge.

8. Sector Notes

8.1 Financial services

Institutions already face stringent supervisory expectations regarding breach reporting, governance and resilience testing. The national cybersecurity agenda is likely to reinforce electronic-evidence preservation and inter-institutional co-operation. Vendors should be subject to equivalent testing and drills.

8.2 Consumer and e-commerce

Narrowed definitions of publicly accessible sources and refined consent mechanics require renewed scrutiny of marketing data acquisition. Privacy notices,

cookie banners and preference centres should align with purpose specificity and retention transparency.

8.3 Health and life sciences

Sensitive data handling and identity flows demand heightened risk assessment, particularly in telemedicine and employee benefits programmes. Clinical and HR governance should be co-ordinated to align access controls, logging and retention with sensitivity and risk.

9. Governance, Rights and Civil Liberties

Centralised digital identity and executive-branch oversight of privacy have prompted a sustained civil-liberties debate. For companies, the most sustainable position is technical neutrality anchored in privacy by design: collect only what is necessary, document proportionality, encrypt thoroughly and enable meaningful user controls.

Data-subject rights (known as ARCO rights) remain formally intact, but procedural expectations may tighten under SABG, particularly in regard to identity verification and response documentation. Automated decision-making remains largely unregulated, increasing the importance of internal safeguards, human-in-the-loop processes, explainability documentation and risk assessments, especially in credit, insurance, employment and mobility contexts.

10. What to Watch For

Key developments to monitor include publication of harmonised LFPDPPP regulations, potential technical corrections to statutory text, and early enforcement signals from SABG. The first judicial decisions from specialised courts will shape practical boundaries regarding consent, notices and accountability.

Digital platforms should begin developing cybersecurity and technical governance standards that allow companies to provide controlled and secure access to their information when required by tax authorities. At the same time, organisations should expect the electronic CURP to become the default mechanism for identifying employees and customers across a wide range of sectors, as Mexico continues to implement biometric-based identity verification. In parallel, companies should anticipate a growing volume of information requests from police and investigative authorities, who, under several of the 2025 reforms, may increasingly rely on corporate datasets for real-time or near-real-time investigative purposes.

Internationally, Mexico's ratification and implementation of the UN Convention against Cybercrime and the outcomes of the USMCA 2026 review will influence electronic-evidence standards, cross-border data governance and AI-related expectations. Organisations that track these developments and maintain disciplined, well-documented governance will be well positioned to adapt incrementally rather than rebuild wholesale.

Mexico's 2025–2026 privacy and cybersecurity environment is dynamic but navigable. Anchor compliance with the new statutory text, interpret consent and notice requirements conservatively, and pre-wire security and incident response programmes for cross-border evidence co-operation. Treat 2026 as a reset year: tighten controls now so future regulatory clarity is a matter of evolution rather than revolution.

MOROCCO

Law and Practice

Contributed by:

Mehdi Kettani, Adil Mouline, Othman Sentissi and Kawtar Mouti
DLA Piper Casablanca

Contents

- 1. Legal and Regulatory Framework p.329**
 - 1.1 Overview of Data and Privacy-Related Laws p.329
 - 1.2 Rights and Obligations p.329
 - 1.3 Special Categories of Personal Data p.330
 - 1.4 Processing of Personal Data for Research and Development Purposes p.330
 - 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.330
 - 1.6 Data Breach Requirement p.330
 - 1.7 Regulators p.330
 - 1.8 Enforcement Proceedings and Fines p.331
 - 1.9 Enforcement Trends p.331
- 2. Privacy Litigation p.331**
 - 2.1 Privacy Litigation Overview p.331
 - 2.2 Recent Case Law p.331
 - 2.3 Collective Redress Mechanisms p.331
- 3. Requirements for the Protection and Processing of Non-Personal Data p.331**
 - 3.1 Objectives and Scope of Data Regulation p.331
 - 3.2 Interaction of Data Regulation and Data Protection p.332
 - 3.3 Rights and Obligations Under Applicable Data Regulation p.332
 - 3.4 Regulators and Enforcement p.332
- 4. Sectoral Topics p.332**
 - 4.1 Use of Cookies p.332
 - 4.2 Personalised Advertising and Other Online Marketing Practices p.332
 - 4.3 Employment Privacy Law p.332
 - 4.4 Data Protection in M&A p.333
- 5. International Considerations p.333**
 - 5.1 Restrictions on International Data Transfers p.333
 - 5.2 Government Notifications and Approvals p.333
 - 5.3 Data Localisation Requirements p.333
 - 5.4 Blocking Statutes p.333
 - 5.5 Recent Developments p.333

DLA Piper Casablanca has three legal specialists and one counsel in its data protection and privacy team, all of whom are able to work in Arabic, English and French. The team regularly assists clients in the context of digital transformation projects, IT regulations queries, and cybersecurity issues. Regarding data privacy specifically, they advise and assist clients in compliance processes relating to data pro-

tection, cross-border data transfers, privacy impact assessments, and vendor management and third-party risk. Some of their relevant work includes drafting and reviewing privacy policies for CFC Authority, Four Seasons Hotels, AIG, FMC Corporation, HCL Technologies, Vivo Mobile Communications, Infobip and TikTok.

Authors



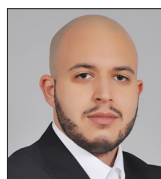
Mehdi Kettani is of counsel at DLA Piper Casablanca. He has assisted clients for more than two decades, both in an advisory and a litigation role, in every field of corporate law (commercial, employment and

intellectual property law), banking and financial law, information technology law and data protection. Mehdi acts mainly for private national and international companies in various industry and service fields such as manufacturing, tourism, energy, transportation and construction, as well as for state-owned entities, banks and financial institutions. Mehdi is admitted to the Casablanca Bar Association.



Adil Mouline is a senior associate in DLA Piper Casablanca's intellectual property and technology team. He has over five years' experience within various advisory firms, which has enabled him to acquire expertise in

different areas of business law, in particular, information technology law, commercial law, corporate law and employment law. Adil advises private national and international companies acting in various sectors such as manufacturing, telecommunications, tourism, distribution, consumer goods, retail services, healthcare and transportation, as well as state-owned entities, banks and financial institutions. Adil is admitted to the Casablanca Bar Association.



Othman Sentissi is an associate in DLA Piper Casablanca's intellectual property and technology team. He has experience in both in-house and outside counsel roles, advising international industry leaders and

disruptive start-ups throughout Africa on various subjects including commercial law, employment law, regulatory law and technology law. Othman focuses on providing innovative legal solutions to enable the implementation of technology-driven business initiatives.



Kawtar Mouti is a mid-level associate at DLA Piper Casablanca who advises Moroccan and international clients on corporate, employment, regulatory and commercial matters. She supports complex transactions,

corporate structuring, workforce management, and compliance with Moroccan legal frameworks, including foreign exchange and data protection regulations. Kawtar assists multinational corporations, private companies and public entities across sectors such as technology, retail, industry and hospitality. Her practice focuses on delivering practical, business-oriented solutions and guiding clients through complex legal and regulatory challenges in evolving markets.

DLA Piper Casablanca

CFC Cube Tower
Casablanca Finance City
Casablanca
Morocco

Tel: +212 520 427 827
Email: sara.essouar@dlapiper.com
Web: www.dlapiper.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Law No 09-08 on the protection of individuals with regard to the processing of personal data and its implementing Decree No 2-09-165 govern personal data in Morocco. This law applies to personal data processing:

- when it is carried out by a natural or legal person established in Moroccan territory; and
- when the data controller is not established in Moroccan territory but uses automated or non-automated means to process personal data in Moroccan territory (except any processing which is used solely for purposes of transit in national territory, or in a country where the legislation is recognised as equivalent to that of Morocco with regard to the protection of personal data).

The regulatory authority in charge of personal data protection in Morocco, the National Commission for the Control of Personal Data Protection (*Commission Nationale de Contrôle de Protection des Données à Caractère Personnel* – CNDP), issues decisions that provide specifications regarding types of processing to simplify the notification requirements and standardise the processing of personal data. Data controllers and processors are required to comply with these decisions. Although Morocco does not yet have AI-specific regulations, the CNDP is currently preparing a decision on AI and personal data.

Data in Morocco is also regulated by Law No 05-20 relating to cybersecurity. This law contains provisions applicable to all data, including but not limited to personal data, processed by specific types of data controllers, such as public entities and critical infrastructures.

In addition to these laws, the EU GDPR and other foreign data protection regulations may apply to some entities in Morocco if the processing conducted by these entities falls within the scope of the regulation in question.

1.2 Rights and Obligations

Moroccan data protection law is built around a set of core principles that shape all personal data processing. Controllers must ensure that data is collected for legitimate purposes, remains proportionate to those purposes, is kept accurate and up to date, and is not retained longer than necessary. Processing typically requires the individual's free, specific and informed consent, except in rare cases allowed by law. Organisations are also required to put in place appropriate technical and organisational safeguards to protect personal data, with reinforced measures when dealing with sensitive personal data.

Individuals are granted a broad range of rights enabling them to understand and control how their personal data is used. These include the right to be informed at the time of collection, the right to access their data, the right to request rectification or deletion of inaccurate or unlawful data, and the right to object to the processing of their data.

To achieve compliance in practice, organisations should implement the following measures:

- map all data-processing activities;
- ensure that all processing activities are conducted within the limits permitted under Moroccan law and regulations;
- ensure that the documentation (eg, information notices and data protection clauses) used in the context of each processing is compliant with the applicable regulations;
- complete mandatory filings with the CNDP or obtain prior authorisations where required, including for sensitive data, changes of purpose or interconnections;
- enter into written contracts with data processors that clearly define security, confidentiality and instruction-bound obligations; and
- implement data retention rules consistent with the purpose of processing.

1.3 Special Categories of Personal Data

Moroccan law imposes enhanced safeguards when processing sensitive personal data, which includes data relating to a person's ethnic or racial origin, political or religious beliefs, trade union membership, health status or genetic characteristics. This data may only be processed under strict conditions and typically requires explicit consent, and prior authorisation from the data protection authority, given its heightened potential to impact individual rights and freedoms.

1.4 Processing of Personal Data for Research and Development Purposes

In Morocco, there are no specific regulations governing the processing of personal data for research and development purposes. As a result, the general data protection rules apply. That said, where anonymisation is effective and the individual is no longer identifiable from the data, the dataset no longer constitutes personal data. In those circumstances, it falls outside the scope of data protection law and may be used without prior authorisation.

Additionally, at the request of the data controller and where a legitimate interest exists, the data protection authority may authorise the retention of personal data for historical, statistical or scientific purposes beyond

the period necessary for achieving the initial purposes of collection.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Morocco does not yet have a dedicated regulatory framework governing artificial intelligence, automated decision-making or algorithmic systems. As a result, any use of personal data in AI models must comply with the general principles of lawfulness, purpose limitation, proportionality and accuracy that apply to all processing activities under Moroccan data protection law. The CNDP is currently preparing a decision that should bring more clarity to the future of AI and personal data in Morocco.

1.6 Data Breach Requirement

Moroccan data protection law requires controllers to implement technical and organisational measures that ensure the security of personal data and protect it against unauthorised access, alteration, disclosure, accidental loss or destruction. These obligations form the foundation of how organisations must prevent data breaches. When a data breach occurs, data controllers and data processors are not required to notify the data protection authority about it under the applicable regulations. That said, notifying the data protection authority about a data breach would be highly recommended.

1.7 Regulators

The CNDP is the only personal data protection regulator in Morocco. The CNDP has jurisdiction over any and all data controllers and data processors that are subject to Law No 09-08 on the protection of individuals with regard to the processing of personal data.

The CNDP has focused, for over a decade, on familiarising stakeholders with the applicable data protection regulations. Over the last few months, the CNDP has started to issue warnings to some major data controllers in Morocco, asking them to comply with the provisions of Law No 09-08. The CNDP has also initiated some investigations into potential violations of the applicable regulations, specifically by data controllers that process significant amounts of personal data.

Cybersecurity on the other hand falls under the scope of a different regulator, which is the Information Systems Security Department within the Ministry of Defence. This regulator is in charge of monitoring, providing guidance and receiving complaints relating to the information systems security of entities that are within the scope of Law No 05-20 on cybersecurity.

1.8 Enforcement Proceedings and Fines

The CNDP has the authority to investigate incidents related to the protection of personal data, and to refer cases to the public prosecutor to initiate proceedings against any suspected offender. In addition to police officers, specially commissioned and duly sworn officers of the CNDP may search for and formally record violations in official reports.

Non-compliance with Law No 09-08 on the protection of individuals with regard to the processing of personal data is subject to a fine ranging from MAD10,000 to MAD600,000 and/or imprisonment of between three months and four years. The CNDP typically sends a warning to the data controller prior to any measure that may result in a fine or imprisonment.

In addition to these fines, legal persons may be punished with one of the following penalties:

- the partial confiscation of their property; or
- seizure of objects and items where the production, use, carrying, holding or selling of such is an offence; or
- the closure of the establishment(s) of the legal person where the offence was committed.

1.9 Enforcement Trends

The CNDP has addressed warning letters to some entities that process large amounts of personal data and/or sensitive personal data. Most of these warnings have been addressed to data controllers such as hotels, pharmaceutical companies, public universities, and other public entities.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Privacy-related litigation in Morocco remains limited, reflecting both the still-developing nature of data protection awareness and the fact that the national authority acts mainly as an educator at this stage.

Individuals may file complaints when their rights to access, rectify or object are denied, and the data protection authority has the power to order corrective measures or refer cases to the public prosecutor for potential criminal proceedings. As a result, many disputes are resolved at the administrative stage, with formal court proceedings arising only when the matter escalates into a criminal offence.

2.2 Recent Case Law

There is no major privacy-related case law in Morocco due to the limited number of litigation cases related to the subject.

Examples of recent court cases do however illustrate an emerging awareness. In one instance, individuals who had been filmed without their consent during the shooting of a movie were awarded damages in court. In another instance, an individual appeared in a company's promotional magazine without having given prior consent and successfully obtained damages in court.

2.3 Collective Redress Mechanisms

There are no privacy-specific collective redress mechanisms in Morocco.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Morocco does not have any non-personal data specific law. The main law that can apply to both personal and non-personal data in Morocco is Law No 05-20 on cybersecurity. It applies to the sensitive information systems owned by a public entity or a critical infrastructure.

Cybersecurity regulations define critical infrastructures as installations, structures and systems that are essential to the maintenance of the vital functions of society, health, safety, security and economic or social well-being, where damage, unavailability or destruction of this infrastructure could result in the failure of these vital functions. The same regulations define public entities as administrations, local authorities, state-owned enterprises and any other legal entity governed by public law.

3.2 Interaction of Data Regulation and Data Protection

Moroccan regulations do not specify how mixed datasets that include personal data and are also subject to the cybersecurity framework should interact. Consequently, the obligations apply cumulatively. Where personal data is involved, Law No 09-08 governs the legal basis and confidentiality requirements for processing. In parallel, Law No 05-20 imposes security and resilience measures on in-scope entities' information systems, irrespective of whether the data is personal or non-personal.

3.3 Rights and Obligations Under Applicable Data Regulation

This is not applicable in Morocco.

3.4 Regulators and Enforcement

The General Directorate of Information Systems Security (*La Direction Générale de la Sécurité des Systèmes d'Information* – DGSSI) is Morocco's national cybersecurity authority, operating under the administration of National Defence. It is responsible for implementing the framework established by Law No 05-20 on cybersecurity, including defining and overseeing organisational and technical measures to strengthen the security and resilience of information systems used by public entities and critical infrastructures.

4. Sectoral Topics

4.1 Use of Cookies

Cookies and similar tracking technologies are regulated only when they collect or contain personal data, such as an IP address or any identifier capable of linking the data to an identifiable individual. In such

circumstances, the deployment of cookies constitutes processing of personal data and becomes subject to the obligations of Law No 09-08, including the requirement to file a notification or obtain prior authorisation from the CNDP, depending on the type and sensitivity of the data being processed. In this context, that data protection authority has issued Decision No D-939-2025 which provides for the possibility of filing a simplified form for specific processing involving cookies.

4.2 Personalised Advertising and Other Online Marketing Practices

Direct marketing by means of automatic calling machines, fax machines, electronic mail or similar technologies is strictly regulated in Morocco. The law expressly prohibits the use of such communication channels when they rely on the contact details of a natural person who has not given their prior and explicit consent to receive promotional messages. Any unsolicited marketing communication using these technologies is therefore unlawful, regardless of the nature of the product or service being promoted.

4.3 Employment Privacy Law

Employers, in the same manner as any other data controller, are required to notify and/or obtain prior authorisation from the CNDP for each purpose for which they process the personal data of their employees.

The processing of employees' personal data specifically for HR management purposes is subject to obtaining authorisation under Decision No 298-AU-2014 of the data protection authority. The decision provides a list of data that may be processed by employers for HR management purposes under a simplified authorisation request. If an employer processes any other data, for the same purpose or any other purpose, they are required to file a separate notification or authorisation request.

Employers are also required to obtain employees' consent for the processing of their personal data and to inform them of the characteristics of the data processing, in accordance with the requirements set out in the applicable Moroccan regulations.

4.4 Data Protection in M&A

In Morocco, personal data processing in M&A transactions is subject to the general obligations of Law No 09-08, meaning that any review or transfer of personal data requires a lawful basis, transparency and adequate security measures. During due diligence, sellers may only disclose personal data that is necessary, proportionate and relevant to the transaction, and must ensure confidentiality through controlled access and contractual safeguards.

If a transaction results in a change of data controller, the new data controller is required to notify the data subjects and the CNDP of said change. Upon notification, the CNDP may require the new data controller to file new declarations and/or authorisation requests.

5. International Considerations

5.1 Restrictions on International Data Transfers

In theory, personal data transfers to countries specified by the data protection authority (see list below) can be completed freely, whereas transfers to any other countries are subject to obtaining authorisation from the same authority.

However, in practice, the CNDP requires prior authorisation to be obtained for data transfers to all countries, with the authorisation being more easily granted if the data is transferred to one of the countries specified in the CNDP's list.

The transfer of personal data abroad requires an adequate level of protection for the privacy and fundamental rights and freedoms of individuals, particularly through standard contractual clauses governing the transfer.

The data protection authority's list of countries is as follows: Austria, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

5.2 Government Notifications and Approvals

Data controllers are required to obtain a separate transfer authorisation for each notified or authorised processing by the CNDP.

5.3 Data Localisation Requirements

Data localisation requirements in Morocco are provided by the cybersecurity regulations and apply exclusively to sensitive information systems owned by a public entity or a critical infrastructure.

5.4 Blocking Statutes

There are no blocking statutes in Morocco.

5.5 Recent Developments

Morocco is continuously working towards joining the list of countries recognised by the EU as providing an adequate level of data protection, but it has not yet obtained a European Commission adequacy decision under the GDPR.

Trends and Developments

Contributed by:

Mehdi Kettani, Adil Mouline, Othman Sentissi and Kawtar Mouti
DLA Piper Casablanca

DLA Piper Casablanca has three legal specialists and one counsel in its data protection and privacy team, all of whom are able to work in Arabic, English and French. The team regularly assists clients in the context of digital transformation projects, IT regulations queries, and cybersecurity issues. Regarding data privacy specifically, they advise and assist clients in compliance processes relating to data pro-

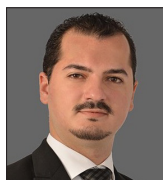
tection, cross-border data transfers, privacy impact assessments, and vendor management and third-party risk. Some of their relevant work includes drafting and reviewing privacy policies for CFC Authority, Four Seasons Hotels, AIG, FMC Corporation, HCL Technologies, Vivo Mobile Communications, Infobip and TikTok.

Authors



Mehdi Kettani is of counsel at DLA Piper Casablanca. He has assisted clients for more than two decades, both in an advisory and a litigation role, in every field of corporate law (commercial, employment and

intellectual property law), banking and financial law, information technology law and data protection. Mehdi acts mainly for private national and international companies in various industry and service fields such as manufacturing, tourism, energy, transportation and construction, as well as for state-owned entities, banks and financial institutions. Mehdi is admitted to the Casablanca Bar Association.



Adil Mouline is a senior associate in DLA Piper Casablanca's intellectual property and technology team. He has over five years' experience within various advisory firms, which has enabled him to acquire expertise in

different areas of business law, in particular, information technology law, commercial law, corporate law and employment law. Adil advises private national and international companies acting in various sectors such as manufacturing, telecommunications, tourism, distribution, consumer goods, retail services, healthcare and transportation, as well as state-owned entities, banks and financial institutions. Adil is admitted to the Casablanca Bar Association.



Othman Sentissi is an associate in DLA Piper Casablanca's intellectual property and technology team. He has experience in both in-house and outside counsel roles, advising international industry leaders and

disruptive start-ups throughout Africa on various subjects including commercial law, employment law, regulatory law and technology law. Othman focuses on providing innovative legal solutions to enable the implementation of technology-driven business initiatives.



Kawtar Mouti is a mid-level associate at DLA Piper Casablanca who advises Moroccan and international clients on corporate, employment, regulatory and commercial matters. She supports complex transactions,

corporate structuring, workforce management, and compliance with Moroccan legal frameworks, including foreign exchange and data protection regulations. Kawtar assists multinational corporations, private companies and public entities across sectors such as technology, retail, industry and hospitality. Her practice focuses on delivering practical, business-oriented solutions and guiding clients through complex legal and regulatory challenges in evolving markets.

DLA Piper Casablanca

CFC Cube Tower
Casablanca Finance City
Casablanca
Morocco

Tel: +212 520 427 827
Email: sara.essouar@dlapiper.com
Web: www.dlapiper.com



Introduction

Personal data protection in Morocco is governed primarily by Law No 09-08 relating to the protection of individuals with regard to the processing of personal data. This law sets the main rules that apply when personal data is collected, stored, used, shared, or combined with other data. In everyday terms, it covers everything from keeping customer contact details, to running a website that remembers user preferences, to managing employee records, to handling medical files. The law is complemented by its implementing decree, Decree No 2-09-165 of 21 May 2009, which clarifies how the law is put into practice and how certain formalities work. Alongside these two texts, the National Commission for the Control of Personal Data Protection (*Commission Nationale de Contrôle de Protection des Données à Caractère Personnel* – CNDP) plays a central role. It is not only an institution that receives notifications and authorisation requests, it is also a body that issues decisions. These decisions translate broad legal principles into practical rules for specific, common situations and, in several cases, they set out simplified notification processes for a defined type of processing.

Why CNDP Decisions Matter

The practical decisions made by the CNDP matter because many of the questions raised by data protection are not abstract. People do not ask about definitions in a law book, they ask what a website may place on their phone, what a company may keep in a visitor log, whether a clinic may use a tool to follow up with patients, or how long a camera recording may be stored. The CNDP decisions answer these ques-

tions by giving a model that data controllers can follow, with clear boundaries. They typically specify the purpose that justifies the processing, the categories of people concerned, and the types of data that may be collected.

The five decisions issued in 2025

During 2025, the CNDP issued five decisions on different subjects, all dated 28 November 2025. Although the topics look diverse, they share a common purpose: to set practical compliance routes for common processing operations that affect a large number of people. The five decisions cover cookies stored on a user device, the management of newsletters, processing for patient follow-up, video surveillance inside healthcare establishments, and the collection of personal data in the context of access control to private professional premises. Read together, they show a regulator that is focused on situations that citizens encounter daily, and on the points where small design choices, such as what a form asks or for how long data is kept, can make a major difference for privacy.

Cookies

The decision on cookies addresses a reality of modern browsing: many websites store small files on a device to remember preferences, measure their audience, or support certain features. The CNDP model treats this as personal data processing when cookies relate to an identifiable person. It then limits the purposes for which the simplified declaration model can be used. Typical purposes that fit within the model include audience measurement and navigation statistics, personalisation of content or services based on previous

choices, and the use of features that allow content to be shared on social networks. At the same time, the CNDP draws a firm line around profiling. If a data controller uses cookie data to build a personal profile of an internet user, such as to determine habits, preferences, or behaviour, the activity then requires prior authorisation. The distinction is easy to understand: counting visits and improving a service is one thing, building a profile of a specific person is another.

The cookie model also turns general principles into precise limits. It sets a maximum retention period of six months for data collected via cookies, after which the data should be deleted or made anonymous. It also deals with consent in a pragmatic way. The model indicates that consent is not required for every cookie purpose, but it is required for certain uses that are more intrusive or commercially sensitive, notably personalised advertising and social network sharing features. Consent must be expressed through a clear action and collected through simple and accessible means offered by the website. Just as important, refusal must be possible and must be respected.

Newsletters

A second decision issued in 2025 focuses on newsletters. Many data controllers send newsletters to customers, members, or the general public, and the processing behind this is often standard: collecting a name and contact details, creating mailing lists, and sending information. The CNDP model sets a simplified declaration route for this activity as long as the data controller stays within a defined parameter. Under the model, the data may be used to constitute and use address lists for external information or communication actions, and to produce statistics related to newsletter campaigns. It is a practical reminder that even common marketing or information activities are still data processing and must follow rules.

Here too, the CNDP highlights a difference that matters in terms of public trust – sending information is not the same as analysing people. The model states that using subscriber data to establish a personal profile requires prior authorisation. In other words, if a newsletter becomes a tool to categorise, predict or influence individuals based on their behaviour, it is treated as higher risk. The decision also sets

straightforward obligations that match what people expect from fair communication. Consent should be obtained, whether through a signature on a paper form or a box that a person actively checks online. Subscribers must be able to unsubscribe at any time through a simple mechanism, such as a link in each message. Data should be kept until the person unsubscribes, which aligns retention with the relationship chosen by the individual rather than with the convenience of the sender.

Patient follow-up

The third decision of 2025 addresses patient follow-ups, a domain where data is essential and where the stakes are high. Health information can reveal intimate details, and misuse can have serious consequences. The CNDP model is designed as a simplified authorisation request for processing used to manage and follow patients. It sets a list of purposes closely linked to care: taking medical appointments, monitoring the state of health of patients, medical diagnosis and therapeutic treatment, producing and communicating analysis results to patients or their legal representatives, following the patient pathway within healthcare establishments, and using telemedicine technologies for care and follow-up. By framing the purposes so tightly, the model emphasises that health data should be processed first and foremost to deliver care, not as a resource to be repurposed without control.

The patient follow-up model also signals that some uses of health data require an even higher level of scrutiny. It states that processing for purposes other than those listed must be subject to specific authorisation. It mentions, among excluded purposes, scientific research that is independent of medical follow-up, as well as the processing of genetic and genomic data. This distinction is important in a context where the line between care and research can become blurred, especially when data can be aggregated and analysed at scale. The model also describes the types of data that may be involved, ranging from identity data and contact details to financial information needed for payment, and of course, medical data concerning the patient's health status. It insists on obtaining consent, informing patients, ensuring security and confidentiality, and controlling transfers abroad, reinforcing the idea that sensitivity calls for discipline at each step.

Video surveillance in healthcare establishments

The fourth decision issued in 2025 concerns video surveillance inside healthcare establishments. Cameras can sometimes play a role in care, for example when constant visual monitoring is necessary for patient safety, but the same cameras can also become intrusive if used without strict limits. The CNDP model applies when a healthcare establishment wants to install a video surveillance system to monitor patients and visitors, and staff who are in contact with these patients and visitors. It limits the processing to specific purposes: surveillance and control of patients, and monitoring interactions between staff and patients and visitors, notably during medical procedures. The framing is significant because it positions the camera system within a care context rather than as a general surveillance tool, while still acknowledging that such processing is sensitive and needs prior authorisation.

The safeguards in the healthcare camera model focus strongly on proportionality. Cameras must only be installed in spaces where constant visual monitoring of patients is necessary, or where medical follow-up requires ongoing visual control to ensure the administration and quality of care. The model also states that installation must not be excessive or intrusive with respect to staff. In particular, it cannot extend to areas reserved for staff and not accessible to patients and visitors, or more broadly, to areas where there is no interaction with patients and visitors. The model also sets a concrete retention rule: recordings should not be kept beyond six months after the patient leaves the establishment, unless another legal rule requires otherwise.

Access control logs

The fifth decision of 2025 deals with access control in private professional premises, a routine that many people experience without thinking of it as data processing. A visitor book at reception, a digital check-in system, or an access badge log can all create a record of who entered a place, when, and for what reason. The CNDP model starts by clarifying that any register or file containing personal data about visitors for access control purposes is personal data processing. It then restricts the acceptable purposes to verifying identity, controlling access, securing the premises and the people and goods inside, keeping time-stamped

entry and exit information, and producing statistics about attendance. These are common sense purposes, but the clarification is important because access control logs can otherwise be quietly expanded into broader monitoring tools.

The access control model also shows how the CNDP applies data minimisation in a concrete way. It lists the data that may be collected, such as the visitor name, the date and time of the visit, the purpose of the visit, and the service and person visited. It sets a maximum retention period of one year unless another legal rule requires longer. Most strikingly, it addresses identity documents. If a security agent asks to see an identity document to verify identity, the model indicates that the agent has no right to retain the document and no right to make a copy. The CNDP considers keeping an identity card number or copying an identity document to be excessive and disproportionate for simple access control, which can be satisfied by consultation without retention.

What these five decisions have in common

Across the five decisions the CNDP repeatedly sets limits on purpose, it narrows what data may be collected, it links retention to necessity, and it insists on transparent information to individuals. It also repeatedly emphasises security and confidentiality and requires that subcontractors offer sufficient guarantees, often through contractual clauses. Finally, it consistently restricts transfers of personal data abroad without prior authorisation. These are not merely bureaucratic steps. They are practical levers that reduce the chance of misuse and the impact of incidents, and they also help create a shared language of trust between data controllers and data subjects.

A decision in preparation on artificial intelligence

In addition to these decisions, the CNDP announced on its website that it was preparing a decision on AI and data protection. In the context of preparatory work, the authority launched auditions and held meetings with different stakeholders, including political parties and professionals working on law, data and related subjects, in order to gather views before issuing guidance on this theme. The CNDP approach, as publicly presented, places emphasis on integrity, transparency, fairness and clarity in AI processing

that uses personal data, and on ensuring that citizens have access to remedies. This upcoming decision is expected to address a subject that is increasingly visible to ordinary people, even when it remains invisible in daily interactions: automated decisions that can shape access to services, prioritisation, recommendations, or risk assessments.

A surveillance decision also announced

The CNDP website also announced that a surveillance decision is in the pipeline. This comes in a context where cameras have multiplied and where surveillance systems can now be connected, searched, and sometimes combined with advanced analytics. Morocco already has a first decision on video surveillance issued in 2013, which addressed the conditions necessary to implement a video surveillance system in workplaces and in private common areas. That 2013 framework set a security purpose as the main justification, required camera placement that avoids intrusion into private spaces, required visible information to people, and limited retention of images to a defined period. A new decision may cover areas that were not covered by the previous text, reflecting how surveillance has expanded in scope and technical capacity.

It may also take a more targeted form, focusing on CCTV cameras within a specific activity, much like the CNDP did in 2025 for healthcare establishments. The healthcare model shows how general technology can be treated differently depending on context, with rules tailored to the sensitivity of the environment and the concrete needs of an activity. A future surveillance decision could similarly clarify what safeguards are required in settings beyond workplaces and private common areas, or it could define stricter conditions for certain uses that raise particular concerns for privacy.

Conclusion

For data controllers, these developments provide more predictable parameters for compliance. The models clarify what is expected and reduce guesswork. For data subjects, they make rights more tangible. A person can better understand why a website asks for consent, why a clinic needs certain information, why a camera should not be placed everywhere, or why a receptionist should not photocopy an identity card. In this sense, the 2025 decisions and the announced work on AI and surveillance underline a basic expectation people have today – that personal data should be used carefully, the reasons for use should be explained, and unnecessary intrusion should be avoided.

NEW ZEALAND



Law and Practice

Contributed by:

Shelley Slade-Gully, Tina Liu, Phil Taylor and Veronica Hartley
Tompkins Wake

Contents

1. Legal and Regulatory Framework p.341

- 1.1 Overview of Data and Privacy-Related Laws p.341
- 1.2 Rights and Obligations p.342
- 1.3 Special Categories of Personal Data p.342
- 1.4 Processing of Personal Data for Research and Development Purposes p.343
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.343
- 1.6 Data Breach Requirement p.344
- 1.7 Regulators p.345
- 1.8 Enforcement Proceedings and Fines p.345
- 1.9 Enforcement Trends p.346

2. Privacy Litigation p.346

- 2.1 Privacy Litigation Overview p.346
- 2.2 Recent Case Law p.346
- 2.3 Collective Redress Mechanisms p.347

3. Requirements for the Protection and Processing of Non-Personal Data p.347

- 3.1 Objectives and Scope of Data Regulation p.347
- 3.2 Interaction of Data Regulation and Data Protection p.348
- 3.3 Rights and Obligations Under Applicable Data Regulation p.348
- 3.4 Regulators and Enforcement p.349

4. Sectoral Topics p.350

- 4.1 Use of Cookies p.350
- 4.2 Personalised Advertising and Other Online Marketing Practices p.350
- 4.3 Employment Privacy Law p.352
- 4.4 Data Protection in M&A p.352

5. International Considerations p.353

- 5.1 Restrictions on International Data Transfers p.353
- 5.2 Government Notifications and Approvals p.354
- 5.3 Data Localisation Requirements p.354
- 5.4 Blocking Statutes p.355
- 5.5 Recent Developments p.355

Tompkins Wake is a leading full-service commercial law firm with more than 120 legal specialists and offices in Auckland, Hamilton, Rotorua and Tauranga. Its privacy and data protection team advises public and private sector clients on regulatory compliance, governance and risk management under the Privacy Act and related legislation. Tompkins Wake supports clients across technology, education, local government, healthcare, financial services and primary industries, reflecting the breadth of its national practice. The firm's work includes privacy impact assessments, data breach response, cross-border

data transfer advice, direct marketing and surveillance issues, information-sharing arrangements and regulatory engagement with the Office of the Privacy Commissioner and the Ombudsman. The team also advises on the intersection of privacy with intellectual property, employment, cybersecurity and technology contracting, ensuring data considerations are embedded in commercial arrangements. Where matters escalate, Tompkins Wake's dispute resolution specialists represent clients in investigations, enforcement proceedings and Human Rights Review Tribunal claims.

Authors



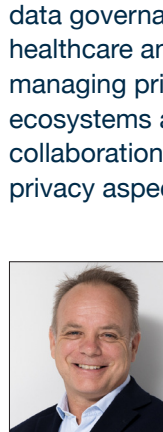
Shelley Slade-Gully is a partner and head of Tompkins Wake's intellectual property and data protection practice. She advises public and private sector clients on privacy compliance under the Privacy Act, data breach

response, regulatory investigations and cross-border data protection issues. Her work includes advising on information-sharing arrangements, surveillance and marketing practices, and the integration of privacy considerations into technology, intellectual property and commercial contracting frameworks. Shelley regularly engages with the Office of the Privacy Commissioner and the Ombudsman on regulatory matters and represents clients in trade mark and data-related disputes before the Intellectual Property Office of New Zealand. She is a member of the Intellectual Property Society of Australia and New Zealand (IPSANZ).



Tina Liu is a specialist in data protection, privacy and regulatory strategy, with a particular focus on the life sciences, healthcare, biotechnology and FMCG sectors. She co-leads Tompkins Wake's

pharmaceutical and biotechnology practice, advising domestic and multinational clients on compliance with the Privacy Act, overseas disclosures of personal and health information, and the structuring of contractual safeguards for global data transfers. Tina provides strategic advice on



Phil Taylor is a partner in Tompkins Wake's corporate and commercial team, with extensive experience advising on cross-border mergers and acquisitions, venture capital investments and complex technology

transactions. He regularly acts on transactions involving data-driven and AI-enabled businesses, where intellectual property and data assets are central to enterprise value. Phil advises on regulatory compliance, foreign investment approvals and the allocation of data protection risk in commercial agreements and corporate structuring. His work includes cross-border acquisitions in the technology and renewable energy sectors across the UK, US, Australia and Asia-Pacific markets.



Veronica Hartley is a senior corporate and commercial lawyer with more than 20 years' experience in private practice and in-house roles across New Zealand, the United Kingdom and Australia. She advises on

complex commercial transactions and technology-driven infrastructure projects, with particular

experience in the energy and telecommunications sectors. Prior to joining Tompkins Wake, Veronica worked in-house at Intellihub Limited, negotiating metering services agreements and acquisitions, and advising on data governance and regulatory compliance within a highly regulated environment. She also brings experience advising on GDPR compliance gained during her time practising in the United Kingdom. Veronica is admitted in New Zealand and England & Wales.

Tompkins Wake

Westpac House, Level 8
430 Victoria Street
Hamilton 3204
New Zealand

Tel: +64 7 839 4771
Fax: +64 7 839 4913
Email: tomwake@tompkinswake.co.nz
Web: www.tompkinswake.com

TOMPKINS | WAKE

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Privacy Act 2020 and Information Privacy Principles

New Zealand's principal data protection law is the Privacy Act 2020 (the "Privacy Act"), which applies across both public and private sectors. It regulates the collection, use, storage, access and disclosure of "personal information" through 13 Information Privacy Principles (IPPs) and provides an oversight and complaints framework administered by the Office of the Privacy Commissioner.

Codes of Practice

The Privacy Act is supplemented by codes of practice issued by the Privacy Commissioner. These codes have the force of law and modify the IPPs for particular sectors or data types. They include the following:

- Health Information Privacy Code 2020;
- Credit Reporting Privacy Code 2020;

- Telecommunications Information Privacy Code 2020; and
- Biometric Processing Privacy Code 2025.

See **5.3 Data Localisation Requirements** for cross-border transfer requirements under these codes.

Right to Privacy

There is no single constitutional "right to privacy" in New Zealand, but privacy interests are protected through multiple instruments. Section 21 of the New Zealand Bill of Rights Act 1990 protects against unreasonable search or seizure, including in relation to correspondence and electronic intrusions. In the public sector, privacy interacts closely with access-to-information regimes governed primarily by the Official Information Act 1982: requests for official information may be refused where withholding is necessary to protect personal privacy.

Extraterritorial Reach

The Privacy Act has material extraterritorial reach. It applies to an overseas agency carrying on business in

New Zealand, regardless of where the personal information was collected or held, or where the individual is located. Cross-border data flows are addressed through IPP 12 (see 5. **International Considerations**).

Interplay With Other Laws

Where data is truly anonymised, it generally falls outside the Privacy Act, though re-identification risk must be carefully managed. Privacy also intersects with cybercrime offences and online harm legislation. Under Part 9A of the Crimes Act 1961, it is a criminal offence to intercept a private communication or to disclose a communication known to have been unlawfully intercepted. The Crimes Act 1961 also creates offences relating to intimate visual recordings made or distributed without consent. Computer-crime offences (including unauthorised access and dishonest use of a computer system) intersect with privacy wherever personal data is involved. New offences targeting software designed for unauthorised access were inserted by the Budapest Convention and Related Matters Legislation Amendment Act 2025 with effect from 31 July 2025. The Harmful Digital Communications Act 2015 provides civil and criminal remedies for harmful online communications and intersects directly with privacy through communication principles prohibiting disclosure of sensitive personal facts or communications made in breach of confidence. New Zealand organisations operating internationally may also need to consider foreign privacy laws with extraterritorial effect (notably the EU GDPR), although New Zealand maintains EU “adequacy” status.

1.2 Rights and Obligations Information Privacy Principles

Under the Privacy Act, organisations must process personal information in accordance with the IPPs. In practical terms, the IPPs require:

- collecting only what is needed for a lawful purpose;
- collecting fairly and generally from the individual;
- providing clear notice at collection;
- maintaining appropriate storage and security safeguards;
- ensuring accuracy before use or disclosure;
- not retaining information longer than necessary;
- limiting use and disclosure to the purpose of collection (subject to exceptions);

- giving individuals access to and the ability to correct their information; and
- applying special controls for unique identifiers and cross-border disclosures.

Data Subject Rights

Individuals have rights to access and request correction of their personal information, and to complain to the Privacy Commissioner regarding an “interference with privacy”. The mandatory breach notification regime requires agencies to notify the Privacy Commissioner and affected individuals where a breach has caused, or is likely to cause, serious harm (see 1.6 **Data Breach Requirement**).

Main Compliance Requirements

Organisations must:

- appoint a privacy officer and maintain a privacy management framework;
- map what personal information they hold, where it sits, and why it is needed;
- use compliant collection notices specifying purpose, recipients, consequences of non-provision, and access/correction processes;
- implement proportionate security safeguards (access control, encryption, logging) and put privacy obligations into vendor agreements;
- validate that secondary uses and disclosures are authorised, particularly for marketing;
- implement processes for access and correction requests (identity verification, timeframes, exemptions); and
- maintain and test a breach response plan covering serious harm assessment, containment, communications and regulator notification.

1.3 Special Categories of Personal Data

New Zealand privacy law does not use the GDPR-style concept of “special category data” with a single heightened processing test. Instead, protection is delivered through the broad definition of personal information, the core IPPs, and sector-specific codes that impose additional controls for inherently sensitive information. The Privacy Commissioner has also issued guidance emphasising that agencies handling sensitive data (broadly, information of real significance to the individual, which is revealing of them or they

would generally wish to keep private) must take extra care and are held to a higher standard of accountability.

Health Information

Health data is regulated by the Health Information Privacy Code 2020, which replaces the IPPs for health agencies and sets more tailored rules for collection, use, disclosure, access and security in clinical and related contexts. This extends beyond traditional healthcare providers to various health-sector bodies and certain entities connected with health services.

Credit, Telecommunications and Biometric Information

Credit information handled by credit reporters is regulated by the Credit Reporting Privacy Code 2020. Telecommunications agencies are subject to the Telecommunications Information Privacy Code 2020, reflecting the sensitivity of communications-related information. The Biometric Processing Privacy Code 2025 regulates organisations using biometrics in automated systems (eg, facial recognition) and phases in compliance for existing uses.

Minors

There is no single “age of consent” threshold in the Privacy Act. However, organisations should treat children’s information as higher risk and ensure collection methods and notices are fair and appropriate. The Health Information Privacy Code expressly highlights fairness considerations where information is collected from children or young persons.

Criminal Convictions

Information about criminal convictions is personal information and subject to the Privacy Act. Additionally, the Criminal Records (Clean Slate) Act 2004 can restrict when conviction history must be disclosed by providing for automatic concealment where eligibility criteria are met (with important exceptions).

1.4 Processing of Personal Data for Research and Development Purposes

Whether patient data may be anonymised for product development or scientific research turns on a threshold question: is the data still “personal information” (ie, about an identifiable individual)? If data is truly

anonymised, it generally falls outside the Privacy Act and Health Information Privacy Code. However, this requires robust controls, as “anonymisation” can fail where datasets can be linked or re-identified.

Legal Gateways for Research

Where information remains identifiable (including pseudonymised data), the relevant privacy rules continue to apply. For companies supplying products or services used by healthcare providers, the key legal gateway is usually the health agency’s authority to disclose information to the supplier and the contractual terms governing that disclosure.

Under the Health Information Privacy Code 2020, health agencies must generally have patient authorisation or rely on a permitted exception. The Code contains a specific pathway allowing disclosure where it is not desirable or practicable to obtain authorisation and the information is to be used:

- in a form in which the individual is not identified;
- for statistical purposes, not published in an identifying form; or
- for research purposes (with ethics committee approval if required), not published in an identifying form.

The Privacy Act IPPs also contain a research and statistics allowance for disclosure where information will not be published in an identifying form, though cross-border disclosures must still satisfy IPP 12 (see 5. International Considerations).

European Health Data Space

The EU Health Data Space Regulation does not apply as New Zealand statute but may affect New Zealand life sciences and digital health companies operating in the EU, supplying health software into EU markets, or seeking to access EU health datasets for research and development.

1.5 Processing of Personal Data in the Context of Artificial Intelligence Privacy Requirements for AI Systems

In New Zealand, the use of personal data in artificial intelligence systems is regulated through existing privacy law rather than AI-specific legislation. The Pri-

privacy Act applies fully to AI-driven processing, meaning organisations must comply with the information privacy principles regardless of whether decisions are made by humans or automated systems. Core obligations include:

- collecting data for a lawful and necessary purpose;
- ensuring accuracy;
- maintaining security safeguards; and
- being transparent about how personal data is used.

Guidance on Automated Decision-Making

While there are no binding AI-specific rules, the Office of the Privacy Commissioner has issued guidance on the use of algorithms and automated decision-making. This guidance focuses on fairness, explainability and accountability. Organisations are expected to understand how AI systems reach decisions, assess risks of bias or error, and ensure individuals can meaningfully challenge or seek review of automated outcomes.

Risk-Based Regulation and International Influence

New Zealand does not operate a formal risk-based AI regime. However, international developments – particularly the EU AI Act – are influencing best practice. Overseas models classify AI systems by risk, prohibit certain uses such as social scoring, and impose heightened obligations on high-risk systems, including strong data governance, transparency and human oversight.

Impact on Data Protection

AI regulation reinforces, rather than replaces, data protection principles. Transparency, responsible data governance and human oversight are increasingly central expectations, especially where AI systems materially affect individuals' rights or interests.

1.6 Data Breach Requirement

Under the Privacy Act, a privacy breach includes unauthorised or accidental access, disclosure, alteration, loss, or destruction of personal information, or any action preventing access to it.

A “notifiable” privacy breach means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely

to do so. The assessment is an objective one, determined from the viewpoint of a reasonable person in the organisation's position who is properly informed based on the information available.

Organisations must notify the Privacy Commissioner and individuals affected by the breach, if the breach is likely to cause serious harm. Organisations should immediately contain (where possible) and mitigate breaches, secure systems and document decisions. A serious harm assessment must be undertaken promptly.

In assessing serious harm, organisations must consider factors such as:

- the nature and sensitivity of the personal information;
- security measures;
- the nature of the potential harm (ranging from physical to financial harm);
- the nature and number of recipients;
- mitigation steps taken to reduce the risk of harm following the breach; and
- other relevant matters.

Notification must occur as soon as practicable after becoming aware a breach has occurred. Notification must cover the prescribed list of details specified in the Act. This includes:

- details of the breach;
- mitigation steps; and
- contact information.

Failure to notify the Privacy Commissioner of a notifiable breach is an offence with a fine of up to NZD10,000.

The Privacy Commissioner has investigative and enforcement powers, including issuing compliance notices. Individuals may bring claims before the Human Rights Review Tribunal, which can award damages. Large breaches may lead to representative actions but are uncommon to date.

1.7 Regulators

Office of the Privacy Commissioner (OPC)

The OPC is an Independent Crown Entity that regulates the Privacy Act. It supervises compliance with the information privacy principles (IPPs), receives mandatory breach notifications, and may issue binding codes of practice, access directions and compliance notices. Complaints are typically raised by individuals after first raising concerns with the relevant organisation, or via notifiable breach reports. The OPC emphasises early resolution but may formally investigate and issue compliance notices where required. Codes of practice and statutory notices are binding; general guidance is influential but not legally binding. See **1.8 Enforcement Proceedings and Fines** for investigation procedure, sanctions and appeal rights.

Human Rights Review Tribunal (HRRT)

The HRRT adjudicates privacy claims, generally after the OPC process, and reviews certain OPC and Health and Disability Commissioner decisions. It may make declarations, restraining orders, performance orders and damages awards. See **1.8 Enforcement Proceedings and Fines** for remedies and penalty bands.

Director of Human Rights Proceedings

The Director of Human Rights Proceedings receives referrals from the OPC where complaints remain unresolved and decides whether to commence proceedings in the HRRT, providing publicly funded representation in appropriate cases.

Health and Disability Commissioner (HDC)

The HDC investigates complaints under the Code of Rights, including confidentiality and health information issues. Matters may be resolved informally or formally investigated; decisions may be reviewed by the HRRT.

Broadcasting Standards Authority (BSA)

The BSA determines broadcast privacy complaints, usually after referral to the relevant broadcaster. It may issue binding determinations, orders and costs awards; appeals lie to the High Court.

Statistics NZ/Government Chief Data Steward

This regulator oversees statistical confidentiality and mandated data standards, which are binding across government. The Data and Statistics Act 2022

includes inspection, compliance notice and criminal offence provisions.

Domestic and Cross-Border Co-Ordination

New Zealand Cabinet Manual guidance requires public sector agencies to consult the OPC on proposals with significant privacy implications. Cross-border, the Privacy Act's complaints framework allows referral of a complaint to an overseas privacy enforcement authority – defined as an overseas body responsible for enforcing personal information protection legislation with investigation and enforcement powers. The Act also contains specific rules governing overseas disclosures under IPP 12 (see **5. International Considerations**).

1.8 Enforcement Proceedings and Fines

An investigation into a privacy breach is initiated when an individual or organisation lodges a complaint with the OPC. The OPC determines whether an investigation is required. If one proceeds, the OPC's primary focus is resolving the matter through settlement or conciliation, a dispute resolution process similar to mediation. The Privacy Commissioner may also act on their own initiative or following a mandatory breach notification. Outcomes include binding access directions and compliance notices, which specify breaches, required steps and timeframes. Compliance notices and access directions are reviewable by the Human Rights Review Tribunal (HRRT). Unresolved matters may also be referred to the Director of Human Rights Proceedings for litigation in the HRRT.

The Tribunal may grant the following:

- declarations;
- restraining orders;
- performance orders; and
- damages for pecuniary loss and humiliation.

Damages awarded can range from NZD3,000 to NZD120,000 and typically fall into three indicative bands:

- up to NZD10,000 for less serious breaches;
- NZD10,000–NZD50,000 for more serious cases; and
- over NZD50,000 for the most serious cases.

These bands are indicative only, as the HRRT ultimately assesses seriousness based on the impact of the breach and any ongoing consequences. Decisions of the HRRT are binding and appealable to the High Court on questions of law.

Criminal offences under the Privacy Act include:

- failure to notify a notifiable breach;
- non-compliance with a compliance notice;
- obstruction; and
- misleading the Commissioner.

Fines are generally up to NZD10,000. Penalties consider seriousness, harm, respondent conduct, mitigation, and general sentencing principles.

Regarding other regulators: the Broadcasting Standards Authority determines broadcast privacy complaints (usually after referral to the broadcaster) and may order apologies, statements, compensation, costs, or fines up to NZD5,000; appeals lie to the High Court. The Health and Disability Commissioner investigates sectoral complaints and may recommend remedies, require action, or refer matters to the Director of Proceedings for proceedings before the HRRT or Health Practitioners Disciplinary Tribunal. Under the Data and Statistics Act 2022, enforcement includes inspections, compliance notices, and criminal offences for unlawful disclosure of statistical information.

1.9 Enforcement Trends

The Privacy Commissioner has reported a significant increase in notifiable privacy breach notifications to its office, with over half of such notifications falling within the classification as involving serious harm. This represents a 47% rise (from previous years) of this type of activity.

Although privacy complaints have increased, this likely reflects both the growing impact of cybersecurity incidents and the greater public awareness of an individual's privacy rights. Private sector notifications to the OPC have more than tripled, indicating that organisations are engaging more actively with their reporting obligations.

While the 2025/26 Annual Report is yet to be released, recent trends show that New Zealanders are increasingly informed about their privacy rights and organisations are responding with greater transparency. The key message for organisations is that expectations around privacy are rising both from the Privacy Commissioner and New Zealanders, and, with cyber threats becoming more sophisticated, strong privacy practices and robust security measures are essential.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Main trends in privacy and data-related disputes specifically before courts can be observed from the High Court decisions of *Neighbourly Ltd v Unknown Defendants* [2026] NZHC 1, *Manage My Health Ltd v Unknown Defendants* [2026] NZHC 2 and *Langley Twigg Partnership v Unknown Defendants* [2026] NZHC 104. In each case, the affected organisations commenced proceedings to urgently contain the consequences of the breach. The key causes of action have been a breach of confidence and breach of privacy, both of which support urgent equitable relief where confidential or sensitive information is at risk.

In each case, the Court was asked to grant injunctions preventing access, use or disclosure of stolen information, reflecting a strong judicial focus on preventing further harm rather than making a determination on liability or compensation. These cases demonstrate that High Court cyber-attack litigation is primarily preventative and protective, rather than compensatory. As a result, non-material damages are not awarded in this particular context, and the courts instead concentrate on securing, controlling and ultimately removing compromised data from being circulated and disclosed.

2.2 Recent Case Law

As described in 2.1 **Privacy Litigation Overview**, the three 2026 High Court decisions of *Neighbourly Ltd v Unknown Defendants* [2026] NZHC 1, *Manage My Health Ltd v Unknown Defendants* [2026] NZHC 2, and *Langley Twigg Partnership v Unknown Defendants* [2026] NZHC 104 collectively establish a consistent judicial framework for cyber-attack litigation in

New Zealand: confidential and sensitive information remains legally protected even after unlawful access, and courts will act swiftly to grant broad injunctive relief to prevent disclosure or further use of stolen data, disrupting cyber-extortion attempts. Together, these decisions confirm that organisations and their clients retain their confidentiality and privacy rights despite a breach and that the courts provide a reliable mechanism for urgent protective relief.

The recent decisions of the Human Rights Review Tribunal, on the other hand, demonstrate a pattern of organisations mishandling personal information in the following ways:

- inadequate information management practices, as in *Jones v Accident Compensation Corporation* [2025] NZHRRT 25;
- failure to respond to information privacy requests, as in *Greensmith v Auckland Council* [2025] NZHRRT 24; and
- disclosing personal information to unauthorised persons, as in *Cummings v KAM Transport Ltd* [2025] NZHRRT 8.

In these cases, the Tribunal has awarded compensatory damages generally between NZD3,500 and NZD30,000, reflective of the harm suffered by the individuals.

2.3 Collective Redress Mechanisms

While privacy and data security issues are likely to form part of the landscape for collective redress, development of collective redress procedure in New Zealand has been in the hands of the courts, with no significant legislative initiatives.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

New Zealand does not have a single overarching statutory framework for the protection and processing of non-personal data. Instead, New Zealand has taken the approach of regulating non-personal data on a sector-specific basis under the Customer and Product Data Act 2025 (CPDA). A key aspect of the CPDA is

the establishment of the Consumer Data Right (CDR) framework, which enables consumers to have greater control over the data they generate.

Outside the CPDA, the protection and processing of non-personal data are generally governed by contracts and laws relating to the protection of intellectual property rights.

How Does It Work?

The CPDA is designation-based. Unless there is a designation regulation enacted under the CPDA for a particular sector, the CPDA would not apply. Currently, under the Customer and Product Data (Banking and Other Deposit-Taking) Regulations 2025 (the “Banking Regulations”), the banking sector is the only industry subject to CDR. The electricity industry is expected to be the next sector to be designated under the CPDA.

The CPDA separates data into two categories:

- “customer data” is data about an identifiable customer held by or on behalf of the data holder, and includes personal information; and
- “product data” relates to the data holder’s product(s) and does not include customer data.

Key actors within the scope of the CPDA include the following:

- data holder – a person specified in a designation regulation who holds designated customer or product data. For example, the Banking Regulations will initially apply to New Zealand’s major banks (ANZ, ASB, BNZ and Westpac), making them the first data holders under the CPDA;
- customer – a person who has acquired, acquires or seeks to acquire goods or services from a data holder; and
- accredited requestor – a third party accredited under the CPDA, allowing them to receive designated data.

The CPDA allows customers or their authorised accredited requestor to request data from a data holder. Customers may then use this data for their own benefit, such as enabling third-party budgeting apps to access the customer’s banking transaction history.

How Does It Compare to the EU Data Act?

The CPDA is materially different in scope and application to the EU Data Act. The CPDA focuses primarily on enabling customer access to, and portability of, data held by designated entities, with regulated accreditation of third-party recipients. In comparison, the EU Data Act goes further by creating mandatory business-to-business (B2B) and business-to-government (B2G) data-sharing rights in certain circumstances. The EU regime also contains detailed provisions on switching between cloud and data processing services and on interoperability, which are not central features of the CPDA.

At the date of publication of this guide (10 March 2026), there is no indication that the New Zealand government intends to enact a law similar to the EU Data Act. It is considered unlikely given the relative size of the New Zealand market compared to that of its major trading partners.

3.2 Interaction of Data Regulation and Data Protection

CPDA and the Privacy Act

The CPDA operates alongside the Privacy Act. Where customer data includes personal information, the data holder must continue to comply with the Privacy Act's Information Privacy Principles (for example, in relation to purpose limitation, security and correction rights), while also meeting any additional data-sharing, portability and accreditation obligations imposed under the CPDA.

The CPDA provides a specific statutory avenue for customers who wish to request access to their designated customer data. However, if the data holder contravenes its obligations to provide the customer with access to their data in accordance with the CPDA, the contravention will be treated as an interference with the privacy of the customer under the Privacy Act.

Further, data holders risk breaching the storage and security of personal information requirements under the Privacy Act if they breach the data storage and security requirements under the CPDA.

CPDA and IP Protection

The CPDA does not displace the operation of existing laws that protect intellectual property rights. During the legislative process, the banking industry emphasised the need to avoid the disclosure of product data that contains commercially sensitive information or information that constitutes a bank's intellectual property.

The CPDA requires the Ministry of Business, Innovation and Employment (MBIE), the government agency responsible for administering the CPDA, to have regard to any intellectual property rights that may exist in relation to customer or product data when designating new classes of customer or product data under any new designated regulations.

3.3 Rights and Obligations Under Applicable Data Regulation

The CPDA (as described in 3.1 Objectives and Scope of Data Regulation) creates a statutory framework for access to and portability of customer data and product data. Under Sections 14 and 15, a customer may request that a data holder provide their designated customer data to them directly, or to an accredited requestor acting on the customer's behalf with the customer's authorisation. The customer may then use that data for their own benefit – for example, authorising a third-party budgeting application to access their banking transaction history held by a participating bank. As noted in 3.1 Objectives and Scope of Data Regulation, the CPDA does not include the switching, interoperability or FRAND provisions found in comparable overseas frameworks such as the EU Data Act; those matters fall outside the current scope of New Zealand's statutory data-sharing framework.

Where a data holder's designated customer data constitutes personal information, the CPDA operates alongside the Privacy Act. A data holder's obligations under Sections 14 and 15 to provide data are separate from, but complementary to, an individual's access rights under IPP 6 of the Privacy Act; requests under the CPDA are expressly not treated as requests under IPP 6 (Section 51 (2) of the CPDA). If a data holder contravenes its obligations to provide data under Section 14, 15 or 16 (2) of the CPDA, that contravention is deemed to be an interference with the privacy of

the individual customer for the purposes of Parts 5 and 6 of the Privacy Act (Section 51 (3)), engaging the Privacy Commissioner's complaint and enforcement jurisdiction.

Action Items for Organisations

Organisations designated as data holders (currently ANZ, ASB, BNZ and Westpac under the Banking Regulations, with the electricity sector expected to follow) should review their obligations under the applicable designation regulations made under Section 104 of the CPDA. The designation framework under Sections 104–107 is sector-expandable: any organisation specified in a future designation regulation will immediately become a data holder. Organisations in sectors likely to be designated should monitor the MBIE's consultation process under Section 106 (which requires consultation with substantially affected persons and the Privacy Commissioner before designation regulations are made) and begin assessing their readiness.

All current and prospective data holders should:

- establish the electronic system required by Section 27 to receive and respond to data requests;
- ensure that system complies with the technical and performance requirements under Section 28;
- implement identity verification processes required by Section 45;
- maintain records under Section 46; and
- audit existing data-sharing practices against both CPDA obligations and the IPPs under the Privacy Act.

Organisations seeking accreditation as accredited requestors should assess their eligibility, the applicable accreditation class, and their obligations under the Privacy Act in respect of any personal information they receive.

3.4 Regulators and Enforcement

Authorities and Enforcement Mechanisms for the Protection and Processing of Non-Personal Data

The CPDA focuses on “product data”, defined in Section 9 as data about or relating to one or more of the data holder's products, but excluding “customer data”. Enforcement primarily concerns the conduct of the “data holder” (defined in Section 6). Section 27

requires a data holder to operate an electronic system capable of receiving requests for regulated data services and providing those services in response. Section 28 prescribes the applicable technical and performance standards that the system must meet.

Non-compliance with Section 28 standards is a civil liability matter under subpart 5 of Part 4 of the CPDA, not a criminal offence. The chief executive may apply to the High Court for a pecuniary penalty order where a data holder has contravened a civil liability provision; maximum Tier 2 penalties are NZD500,000 for an individual or NZD2.5 million in any other case. A separate criminal offence arises under Section 30 only where a data holder fails to comply with a written notice from the chief executive requiring it to test its electronic system under Section 29 (or gives a false or misleading test report), carrying fines of up to NZD100,000 for an individual or NZD300,000 in any other case.

Additional enforcement mechanisms are set out in Part 4. Section 53 empowers the chief executive (being the chief executive of the MBIE) to require any person, by written notice, to supply information or produce documents. The exercise of that power is subject to Section 56, which requires destruction of information obtained through any exercise of Section 53 powers that is subsequently declared unlawful by a court. Failure to comply with a Section 53 notice, or supplying false or misleading information in purported compliance, is a criminal offence under Section 57, carrying fines of up to NZD100,000 for an individual or NZD300,000 in any other case.

Under Section 44, it is a criminal offence for a person to knowingly request a regulated data service that relates to a customer when not permitted to do so; an individual is liable to imprisonment for up to five years or a fine of up to NZD1 million (or both), and a body corporate to a fine of up to NZD5 million.

Subpart 2 of Part 4 addresses remedial obligations. Section 58 requires a data holder or accredited requestor to take the steps prescribed by the regulations to avoid, mitigate or remedy loss or damage suffered by a customer or another data holder or accredited requestor as a result of a contravention. Section 59 provides that an amount required to be paid under

those regulations may be recovered as a debt in any court of competent jurisdiction.

Co-Ordination With the Privacy Commissioner

The CPDA contains two express bridges to the Privacy Act's enforcement regime. Under Section 51 (3), if a data holder contravenes Section 14, 15 or 16 (2) – failing to provide designated customer data as required – that contravention is treated as an interference with the privacy of the individual customer for the purposes of Parts 5 and 6 of the Privacy Act, giving the Privacy Commissioner jurisdiction to receive and investigate complaints and the Human Rights Review Tribunal jurisdiction to award remedies. Under Section 52, if a data holder contravenes a CPD storage and security requirement in relation to personal information, it is treated as breaching IPP 5 of the Privacy Act, again engaging the Privacy Commissioner's enforcement role. The Minister must also consult the Privacy Commissioner before recommending designation regulations under Section 106. These mechanisms mean that enforcement of the CPDA will, in practice, engage both the chief executive's civil enforcement powers and the Privacy Commissioner's jurisdiction in parallel.

Given the recent enactment of the CPDA, no enforcement actions have yet been taken and no trends have emerged. As the Banking Regulations take effect and the first data requests are processed, enforcement patterns – and the practical interaction between the chief executive's powers and the Privacy Commissioner's jurisdiction – are expected to become clearer in the next 12 to 24 months.

4. Sectoral Topics

4.1 Use of Cookies

New Zealand does not have specific legislation governing cookies, software development kits or other online tracking technologies comparable to the EU's ePrivacy Directive or the UK's Privacy and Electronic Communications Regulations, and there is no statutory opt-in consent or opt-out model for tracking technologies. However, the Privacy Act applies directly where tracking technologies collect or generate information about an identifiable individual.

The key applicable principles are as follows. IPP 1 requires that personal information be collected only for a lawful purpose connected to the agency's functions, and only to the extent necessary; meaning speculative data harvesting or collection without a clear purpose is unlikely to be compliant. IPP 3 requires that, where personal information is collected from an individual, the agency takes reasonable steps to ensure the individual is aware of the fact of collection, the purpose, the intended recipients, and the identity of the collecting agency; this effectively requires websites and applications using tracking technologies to maintain an accurate and accessible privacy or cookie notice. IPP 4 requires collection by fair and lawful means without unreasonable intrusion on personal affairs, which applies directly to covert or opaque tracking. IPP 10 prohibits use of personal information collected for one purpose (such as analytics) for a materially different purpose (such as targeted advertising or sale to data brokers) without a lawful basis, which, in practice, generally requires individual consent.

There is no "cookie consent" requirement equivalent to the General Data Protection Regulation or ePrivacy Directive framework. However, the Privacy Commissioner has indicated that organisations relying on tracking technologies for purposes beyond what individuals would reasonably expect should review their compliance with IPPs 1, 3 and 10, and ensure their privacy notices are accurate and accessible. Where electronic messages are sent using data gathered through tracking, the Unsolicited Electronic Messages Act 2007 applies. The Fair Trading Act 1986 applies to the extent that tracking-based advertising involves misleading or deceptive conduct.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised or targeted advertising is regulated in New Zealand primarily by the following:

- Privacy Act 2020 and associated privacy codes;
- Unsolicited Electronic Messages Act 2007 (UEMA); and
- Fair Trading Act 1986 (FTA).

Advertising codes of conduct may also apply. Certain content within personalised or targeted advertising

may be subject to specific legislation (eg, where content constitutes financial advice, the Financial Markets Conduct Act 2013 will apply).

Privacy Act 2020

The Privacy Act applies to the collection and use of personal information for personalised advertising on the same basis as described in **4.1 Use of Cookies**. In particular, IPP 10 restricts use of data collected for one purpose (such as website analytics or account management) for an unrelated purpose such as targeted advertising and use for the latter purpose will generally require the individual's consent. Organisations must also ensure that their data collection practices for advertising purposes comply with the transparency requirements of IPP 3 and the purpose-limitation requirement of IPP 1, as described in **4.1 Use of Cookies**.

The Unsolicited Electronic Messages Act 2007 (UEMA)

The UEMA governs “commercial electronic messages” and applies to, among other things, marketing and promotional material sent through an electronic message (including SMS or email) for the promotion of goods or services.

The UEMA provides that a person must not send, or cause to be sent, “an unsolicited commercial electronic message that has a New Zealand link” without consent (as discussed further below). Consent is therefore required to send personalised or targeted commercial electronic messages.

In addition to the requirement for consent, commercial electronic messages must identify the sender and have an unsubscribe facility.

Fair Trading Act 1986 (FTA)

The FTA provides broad protection to consumers from, among other things, misleading, deceptive and unfair conduct. While the FTA does not specifically regulate personalised or targeted advertising, the conduct of advertisers must comply with the FTA. A personalised advertisement may breach the FTA if, for example, it contains claims suggesting a product suits a consumer's specific individual requirements which cannot be substantiated.

Industry Codes

Industry codes including the ASA Advertising Standards Code and Children's Advertising Code set standards for advertising in New Zealand. While compliance with these codes is not a legal requirement, in practice there is a high level of compliance in New Zealand due to contractual requirements of many media outlets, and non-compliance with these standards indicates possible non-compliance with the requirements of the FTA.

Profiling

There is no specific regulation of profiling for the purpose of personalising or targeting advertising in New Zealand. However, in the course of profiling, the advertiser would need to comply with the Privacy Act requirement that collection of personal information must be for a lawful purpose and that, in the circumstances (particularly in relation to children and young persons), the collection is fair and does not intrude unreasonably upon the personal affairs of the individual.

For any profile created that contains personal information, the Privacy Act requires that the profiling agency takes reasonable steps to ensure the information is accurate, up to date, complete, relevant and not misleading.

Sensitive Data

The Privacy Act does not have an express “sensitive information” category. However, certain types of personal information are treated as “sensitive” under the Privacy Act. For example, the Health Information Privacy Code 2020 (issued under the Privacy Act) places additional privacy safeguards on the collection, use and disclosure of health information.

Information collected from children and young people is also regulated under the Privacy Act. While the Privacy Act does not have specific provisions relating to the privacy rights of children and young persons, the Act highlights that particular considerations must be given to ensure that the manner of collection must be fair and not unreasonably intrude on the personal affairs of the child or young persons.

In addition to the ASA Advertising Standards Code, discussed above, a separate code, the Children's Advertising Code, applies to advertising targeted to children.

Consent Requirements

Consent to use personal information for personalised or targeted advertising is not required under the Privacy Act, provided the information is collected for a lawful purpose and collection is necessary for that purpose, the individual has been informed of the collection and the purpose of collection, and certain other conditions are satisfied.

Children may lack capacity to provide adequate consent for collection and use of their personal information, and consent from a parent or guardian will generally be required. As discussed above, the UEMA requires consent to commercial electronic messages and is also applicable to targeted and personalised commercial electronic messages sent to children.

Consent to commercial electronic messages may be express, inferred or deemed from circumstances. The person claiming that a recipient has consented to receiving a message has the onus of proving that consent was provided. There is no prescribed form for obtaining consent.

Targeted online advertising that appears on social media platforms is not subject to the UEMA, unless it involves the sending of an electronic message to the viewer.

4.3 Employment Privacy Law

In New Zealand, employment privacy is primarily governed by the Privacy Act, alongside the Employment Relations Act 2000 (good faith obligations), the Human Rights Act 1993 (non-discrimination), and, where relevant, the Health and Safety at Work Act 2015.

Employers may collect employee or applicant information only for a lawful and necessary purpose connected with their functions (IPP 1). Under IPP 3, individuals must be informed of the following:

- purpose of collection;
- intended recipients;

- consequences of non-provision; and
- their rights of access and correction.

These principles apply equally to recruitment. Regarding prospective employees, background checks must be necessary, transparent and non-discriminatory.

Employee monitoring is permitted but must be lawful, necessary, transparent and not unreasonably intrusive. Employers should clearly inform staff of monitoring practices. Such practices must also comply with employment law good faith and procedural fairness requirements.

For remote work, IT systems and BYOD, employers remain responsible for ensuring reasonable security safeguards of personal information, including secure access controls and protection against unauthorised disclosure. Where third-party or cloud providers are used, the employer remains accountable, and cross-border disclosures must comply with IPP 12.

Serious employment-related data breaches trigger mandatory notification obligations and potential liability, including damages for humiliation or injury to feelings.

4.4 Data Protection in M&A

Mergers and acquisitions in New Zealand are likely to engage privacy obligations at every stage, as follows.

Due Diligence

During due diligence, the target is likely to disclose personal information about employees, customers and suppliers to the acquirer. IPP 11 (1)(i) provides a specific gateway, permitting disclosure where necessary to facilitate the sale or disposition of a business as a going concern. This exception operates without individual consent but applies only where the transaction genuinely involves disposing of a business as a going concern, not merely asset sales or partial disposals.

Despite this statutory exception, organisations should implement robust controls:

- limiting disclosure to information genuinely necessary;

- restricting access through NDAs and data rooms;
- anonymising data where feasible; and
- delaying transfer of highly sensitive information until completion.

Change of Control and Integration

At completion, personal information transfers to the acquiring entity/agency. This is generally permissible as information continues to be used for purposes directly related to the original collection. However, agencies must update privacy notices to reflect the change in agency, align security measures across the combined entity, and review retention policies.

Cross-Border Considerations

Where an acquirer or merged entity is located offshore, or information will be hosted overseas post-transaction, IPP 12 requires specific safeguards for cross-border disclosures, including obtaining individual authorisation, confirming comparable privacy protections or implementing contractual safeguards.

Notification

There is no general obligation to notify individuals or the Privacy Commissioner purely due to change of control, though good practice involves updating privacy statements promptly.

5. International Considerations

5.1 Restrictions on International Data Transfers

Disclosure Outside New Zealand

IPP 12 of the Privacy Act governs “disclosure” of personal information outside New Zealand. Disclosure is not defined in the Privacy Act but given its usual meaning will apply to an agency subject to the Act making the personal information available to a third party. This will include transfers of information unless an exception applies under the Act.

Personal information may only be disclosed outside New Zealand where the disclosing agency has first ensured that appropriate safeguards apply.

In practical terms, before disclosing personal information overseas, the agency must take reasonable steps to confirm that the overseas recipient:

- is carrying on business in New Zealand and therefore subject to the Privacy Act; or
- is subject to privacy laws that, overall, provide comparable safeguards to the New Zealand regime; or
- is contractually required (for example, through appropriate data protection clauses) to protect the information in a way that provides comparable safeguards.

If none of these safeguards apply, the information may only be disclosed if the individual expressly authorises the disclosure after being clearly informed that the overseas recipient may not be required to protect their information to the same standard as under the New Zealand Privacy Act.

Onward Transfers

Onward transfers of information, after the initial overseas disclosure, are governed by the contractual arrangement between the NZ agency and the overseas recipient relating to the initial data disclosure. While the Privacy Act does not prescribe any “model clauses” that must be included in a data transfer agreement, the New Zealand Privacy Commissioner provides a set of “off the shelf” clauses that can be voluntarily used to ensure that the data transfer agreement contains the necessary privacy safeguards comparable with the Privacy Act.

Exceptions

The requirements relating to the overseas disclosure of personal information do not apply where the disclosure by an agency is to a service provider and the information will be held by the service provider for storing or processing solely on behalf of that agency, and the service provider will not use the information for its own purposes.

In such circumstance, the Privacy Act does not treat the disclosure of personal information to be an overseas disclosure, and instead treats the information as being held by the agency (even where the information is actually stored outside New Zealand).

Non-Personal Data

There is no general regulation applicable to the transfer or other disclosure of non-personal information outside New Zealand.

5.2 Government Notifications and Approvals

New Zealand does not require organisations to register, file or obtain prior approval from any authority before making international transfers of personal information. The applicable framework under IPP 12 of the Privacy Act imposes substantive transfer-restriction obligations on the disclosing agency (see **5.1 Restrictions on International Data Transfers**), but compliance with those obligations is self-assessed and does not involve any prior notification to or authorisation by the Privacy Commissioner or any other regulator. No binding scheme regulations or prescribed country regulations have been made under Section 213 or 214 of the Privacy Act as at the date of publication of this guide. New Zealand has no export control regime applying to data transfers as such, and no equivalent of Article 32 of the EU Data Act.

5.3 Data Localisation Requirements

Data Localisation Requirements

New Zealand does not impose general statutory data localisation or residency requirements. There is no blanket prohibition on storing or processing personal information offshore.

Cross-Border Transfer Framework

IPP 12 governs disclosure of personal information outside New Zealand. Before disclosing personal information to foreign persons or entities, agencies must meet specified safeguards, including the following:

- individual authorisation with express notification that offshore protections may differ;
- the recipient being subject to the Privacy Act (by carrying on business in New Zealand);
- the recipient being subject to privacy laws providing comparable safeguards;
- the recipient being a participant in a prescribed binding scheme; or
- the agency otherwise ensuring comparable protections through contractual or other means.

Complementing this, Section 11 of the Customer and Product Data Act 2025 imposes requirements for the standardised handling of customer and product data, applying to New Zealand agencies wherever they operate and to overseas agencies conducting business in New Zealand, regardless of where the data is located.

Remote Access

The Privacy Act does not distinguish between transferring information offshore and granting remote access to information held in New Zealand from an offshore location. Both are regulated under IPP 12.

Sector-Specific Codes

Section 32 of the Privacy Act enables the Privacy Commissioner to issue codes of practice that may modify the application of one or more IPPs. The Health Information Privacy Code 2020, Biometric Processing Privacy Code 2025, Telecommunications Information Privacy Code 2020, and Credit Reporting Privacy Code 2020 each apply IPP 12's cross-border safeguards to certain sector-specific disclosure grounds and require that offshore recipients provide protections comparable to those in the Privacy Act as modified by the relevant code.

The Civil Defence National Emergencies (Information Sharing) Code 2020 makes IPP 12 compliance subject to reasonable practicability during national emergencies.

None of the codes imposes data localisation or residency requirements.

Practical Implications

While there is flexibility to use offshore infrastructure and service providers, agencies must conduct transfer impact assessments, implement contractual protections with offshore processors, and maintain documentation demonstrating IPP 12 compliance. Sector-specific codes may require additional safeguards depending on the type of information being transferred.

5.4 Blocking Statutes

Blocking Statutes

New Zealand has not enacted a broad or comprehensive blocking statute equivalent to those operating in other jurisdictions, such as Council Regulation (EC) No 2271/96 (the “EU Blocking Statute”), which expressly prohibits EU persons from complying with specified extraterritorial US sanctions, or China’s Data Security Law and Personal Information Protection Law, which prohibit provision of data to foreign judicial or law enforcement authorities without prior state approval. Instead, New Zealand’s framework addresses cross-border issues through controls on the transfer of personal information and domestic implementation of international sanctions obligations.

Gathering Evidence for Foreign Proceedings

For foreign civil proceedings, Sections 184–185 of the Evidence Act 2006 provide a mechanism by which the High Court may order the examination of witnesses, production of specified documents, inspection of property, or other evidence-gathering steps if requested by a foreign court. For foreign criminal matters, the Mutual Assistance in Criminal Matters Act 1992 (MACMA) enables foreign governments to request evidence-gathering assistance from New Zealand via the Attorney-General, subject to mandatory and discretionary grounds for refusal. Both regimes preserve standard New Zealand witness privileges and compellability rules, and the MACMA expressly preserves the operation of the Evidence Act 2006.

Sanctions Compliance

The United Nations Act 1946 empowers the Governor-General, by Order in Council, to give effect to UN Security Council measures; sanctions apply in New Zealand only once implementing regulations are made. New Zealand does not restrict entities from voluntarily complying with foreign sanctions regimes, provided such compliance does not contravene domestic law.

Cross-Border Disclosures and Privacy

The Privacy Act operates as New Zealand’s primary constraint on offshore disclosure of personal information through IPP 12 (see **5.1 Restrictions on International Data Transfers**). Even without a blocking statute, privacy law can limit compliance with foreign

discovery requests where personal information is involved.

Māori Data Sovereignty

Where Māori data is involved, organisations should give practical consideration to Māori Data Sovereignty principles (Te Mana Raraunga) and may face ethical obligations to consult iwi or hapū before releasing information offshore, even where IPP 12 would otherwise permit the transfer.

5.5 Recent Developments

New Zealand’s Adequacy Status Reaffirmed

In 2024, the European Commission reaffirmed New Zealand’s adequacy status, confirming that New Zealand’s level of personal data protection is comparable to Europe’s standards. This is significant because it allows the transfer of personal data about EU residents, to New Zealand, without additional safeguards under EU law. The reaffirmation of New Zealand’s status signals to the world continued confidence that New Zealand’s privacy framework supports cross-border trade in an increasingly data-driven world.

As part of the process for New Zealand to retain its adequacy status, the New Zealand government introduced, in the recent Privacy Amendment Act 2025, a new principle (IPP 3A) to the Privacy Act. IPP 3A concerns the indirect collection of personal information. It requires that if an agency collects personal information indirectly (eg, a lender obtains credit history information from a credit reporting agency or an employer obtains references about an applicant from a former employer), the agency must inform the individual concerned, unless an exception applies.

Previously, there was no notification requirement for the indirect collection of personal information. This gap in New Zealand’s privacy framework was highlighted during the EU’s assessment of New Zealand’s “adequacy status”.

Overseas Transfer

Principle 12 of the Privacy Act regulates the disclosure of personal information to organisations or people outside New Zealand. Among the different pathways in IPP 12 to permit the disclosure of data overseas,

it provides that some disclosures can be simplified if the recipient is subject to:

- a prescribed binding scheme; or
- the laws of a prescribed country.

However, to date, there are no regulations prescribing binding schemes or countries for the purpose of IPP 12.

Furthermore, the amendments to IPP 12 (1)(e) by the Statutes Amendment Act 2025 indicate that, even if there were to be a regulation prescribing a country or a binding scheme, the transfer of data may be subject to limitations or qualifications prescribed in regulations in respect of the overseas disclosure to that country.

In the meantime, as set out in **5.1 Restrictions on International Data Transfers**, an agency seeking to disclose data outside New Zealand can use the other pathways set out in IPP 12 for the overseas disclosure.

PAKISTAN



Law and Practice

Contributed by:

Saifullah Khan and Saeed Hasan Khan
S.U.Khan Associates

Contents

1. Legal and Regulatory Framework p.359

- 1.1 Overview of Data and Privacy-Related Laws p.359
- 1.2 Rights and Obligations p.359
- 1.3 Special Categories of Personal Data p.360
- 1.4 Processing of Personal Data for Research and Development Purposes p.361
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.361
- 1.6 Data Breach Requirement p.361
- 1.7 Regulators p.361
- 1.8 Enforcement Proceedings and Fines p.361
- 1.9 Enforcement Trends p.362

2. Privacy Litigation p.362

- 2.1 Privacy Litigation Overview p.362
- 2.2 Recent Case Law p.362
- 2.3 Collective Redress Mechanisms p.362

3. Requirements for the Protection and Processing of Non-Personal Data p.362

- 3.1 Objectives and Scope of Data Regulation p.362
- 3.2 Interaction of Data Regulation and Data Protection p.362
- 3.3 Rights and Obligations Under Applicable Data Regulation p.362
- 3.4 Regulators and Enforcement p.362

4. Sectoral Topics p.362

- 4.1 Use of Cookies p.362
- 4.2 Personalised Advertising and Other Online Marketing Practices p.363
- 4.3 Employment Privacy Law p.363
- 4.4 Data Protection in M&A p.363

5. International Considerations p.363

- 5.1 Restrictions on International Data Transfers p.363
- 5.2 Government Notifications and Approvals p.364
- 5.3 Data Localisation Requirements p.364
- 5.4 Blocking Statutes p.364
- 5.5 Recent Developments p.364

S.U.Khan Associates is a pioneering and leading firm practising trade remedy law in Pakistan, with local and international clients. Its major service areas include international trade laws, data protection, e-commerce and IT laws, competition law, customs and taxation, corporate, foreign investment advisory and international trade agreements advisory. The firm is also a great contributor to the dissemination of professional knowledge in various journals, as well as to international institutions such as the United Na-

tions Conference on Trade and Development and the United Nations Commission on International Trade Law (UNCITRAL). S.U. Khan Associates' partners have been working closely with the government of Pakistan in drafting legislation and in policy-making. The firm advises clients on compliance requirements related to personal data protection, preparation and review of policies and agreements concerning data privacy and transfer of data.

Authors



Saifullah Khan is an international trade, IT and policy lawyer with more than 23 years of diversified and multi-jurisdictional professional experience in serving a large client base in the domestic and international

markets. His areas of interest include WTO trade remedy laws, customs law, competition law and data privacy. Regarding the emerging discipline of data privacy, he advises clients from different jurisdictions about data privacy compliance and cross-border transfer of data. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".



Saeed Hasan Khan has more than 23 years' experience in advising and representing clients on issues such as taxation, corporate, regulatory compliance and contractual obligations. He has developed a keen

professional interest in emerging laws on personal data protection, and an understanding of the underlying concepts and principles governing global data protection laws, including the EU's GDPR. He has carried out considerable research on personal data protection laws in various jurisdictions. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK), holds CIPP/E certification and is a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

S.U.Khan Associates, Corporate and Legal Consultants

First Floor, 92-Razia Sharif Plaza
Fazal-ul-Haq Road
Blue Area
Islamabad
Pakistan

Tel: +92 51 2344 741
Fax: +92 51 2344 743
Email: saeed.hasan@sukhan.com.pk
Web: www.sukhan.com.pk



S.U.Khan Associates
Corporate & Legal Consultants

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Constitution of Pakistan, under Article 14, recognises the right to privacy as a fundamental right. In this context, the Ministry of Information Technology and Telecommunication has prepared a draft Personal Data Protection Bill, 2023 (the “Draft Bill”). Although the Draft Bill has completed the consultation stage, it has yet to be passed by both houses of the Parliament. Its framework largely mirrors the European Union’s General Data Protection Regulation (GDPR).

Pakistan is also a signatory to the International Covenant on Civil and Political Rights (ICCPR), which also demands that signatory states protect the privacy of individuals.

Sector-specific laws or regulations are enforced in Pakistan, specifically governing privacy of customers/individuals in the respective sectors.

The Pakistan Telecommunication Authority (PTA), under the Pakistan Telecommunication (Re-Organization) Act, 1996, issued the Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009. These regulations apply to all telecommunications operators and are designed to safeguard consumers from spam, fraudulent, unsolicited and obnoxious communications. The Prevention of Electronic Crimes Act, 2016 (PECA), addresses cybercrime, offering protection against electronic offences and fraud involving personal or digital data, and seeks to protect the integrity, privacy and security of electronic data.

The Banking Companies Ordinance, 1962, governs the banking sector in Pakistan. It requires that banks not disclose any information pertaining to consumers’ data except where required under the law or for an appropriate purpose. Similarly, the Payment Systems and Electronic Fund Transfers Act, 2007 (the “Electronic Fund Transfers Act”), regulates electronic fund transfers and consumer protection, secrecy and privacy.

The Credit Bureaus Act, 2015, and the regulations made thereunder govern the unauthorised access or disclosure of credit information.

The Right of Access to Information Act, 2017, governs the general public’s right to access information; however, no such information will be provided that jeopardises the privacy of an identifiable individual. In Appeal No 1080-05-2021, the Pakistan Information Commission held that an appellant seeking information concerning a housing society was entitled to receive the requested material, provided that any information affecting the privacy of other members was redacted. In its E-Commerce Policy of Pakistan (2019) and elsewhere, the Ministry of Commerce has adopted data protection as one of its policy initiatives.

With regard to the extraterritorial scope of the Draft Bill, it provides that personal data must not be transferred to any unauthorised person. Critical personal data may only be processed on servers located within Pakistan, while the Commission is tasked with devising a mechanism for the transfer of sensitive personal data. Where personal data, other than critical or sensitive personal data, is to be transferred outside Pakistan, the receiving country must have an adequate legal framework for personal data protection. In the absence of such adequacy, the Commission may authorise the transfer subject to specified safeguards, including:

- binding contractual arrangements;
- the explicit consent of the data subject provided such consent does not conflict with Pakistan’s public interest or national security;
- transfers necessary for international co-operation pursuant to applicable international obligations; and
- any additional conditions prescribed by the Commission.

1.2 Rights and Obligations

Grounds for Processing Personal Data

- Lawful and Fair Processing: Personal data must be processed in a lawful, transparent, and fair manner, in compliance with the Act.
- Purpose Limitation and Legitimate Purpose: Data may only be collected for specified, explicit, and

legitimate purposes and must not be further processed in a way that is incompatible with those purposes.

- **Data Minimisation:** The data collected must be adequate, relevant, and limited to what is necessary to achieve the stated processing purpose.
- **Regulatory Registration:** Data controllers and processors operating in Pakistan must register with the Commission in the prescribed manner or notify the Commission if already registered with another public authority.
- **Appointment of Data Protection Officer:** Data controllers or processors classified as “significant” by the Commission must appoint a data protection officer with adequate knowledge of personal data processing and related risks.

Rights of Data Subjects

The Draft Bill provides the following rights to data subjects:

- **Right to Access:** A data subject has the right of access to their personal data and may obtain confirmation from a data controller as to whether their personal data is being processed or has been processed.
- **Right to Correction:** A data subject may make a data correction request in writing to a data controller or data processor.
- **Right to Withdraw Consent:** A data subject may withdraw his/her consent by giving a written notice.
- **Right to Prevent Processing Likely to Cause Damage or Distress:** A data subject has the right to prevent the processing, subject to certain conditions, by providing a data subject notice.
- **Right to Erasure:** A data subject has the right to request that the data controller erase his/her personal data without undue delay.
- **Right to Nominate:** A data subject has the right to nominate anyone to exercise his/her rights in the event of death or disability.
- **Right to Redressal of Grievance:** A data subject may file a complaint with the data controller, and in case where a data controller fails to resolve his/her grievance, the data subject may file a complaint with the Commission.
- **Right to Data Portability and Automated Processing:** A data subject shall have the right to receive

his/her personal data from the data controller in a proper form, and the right not to be subject to a decision based solely on automated processing.

Compliance “To Dos”

As Pakistan’s Personal Data Protection Bill is still in draft form, its provisions do not yet offer a complete or enforceable compliance framework. In this interim period, it is prudent for organisations to align their data protection practices not only with the principles reflected in the Draft Bill, but also with established international best practices, particularly those embodied in the GDPR, to ensure a higher level of data protection, regulatory readiness, and future compliance once the law is enacted.

1.3 Special Categories of Personal Data

Under the Draft Bill, sensitive and critical personal data may only be processed on an exceptional basis. Generally, explicit consent of the data subject is required, provided such consent is not restricted by any other applicable law. In addition, processing is permitted only when one of the following conditions is met:

- where it is necessary for clearly defined purposes, including employment-related legal rights and obligations,
- for protection of vital interests where consent cannot reasonably be obtained;
- for medical purposes subject to confidentiality;
- for legal proceedings and legal advice;
- for the establishment or defence of legal rights;
- for administration of justice under court orders, or the exercise of functions conferred by law; and
- where the data has been deliberately made public by the data subject.

The Commission retains the power to impose additional conditions or restrict the application of certain grounds through orders published in the Gazette.

Children’s Personal Data Processing

Personal data relating to a child must be processed in a way that safeguards the child’s rights and best interests. Before processing such data, data controllers and processors are required to verify the child’s age and obtain consent from a parent or legally authorised guardian in accordance with rules prescribed by law.

Children's data must not be processed in a manner that may cause harm, and practices such as tracking, behavioural monitoring, or targeted advertising directed at children are prohibited. Limited exceptions may apply where processing is permitted for specific purposes prescribed under the Act.

1.4 Processing of Personal Data for Research and Development Purposes

As Pakistan does not currently have an effective, dedicated legal framework governing the processing of personal data for research and development purposes, no specific statutory conditions have been formally prescribed in this regard. Nevertheless, companies that provide products or services used by healthcare providers must exercise particular caution when handling personal data, whether in its original form or after anonymisation, and should adhere to internationally recognised best practices. In particular, organisations must ensure that any data relied upon for research or development is irreversibly anonymised, such that it can no longer be used to identify a patient, either directly or indirectly.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

In 2023, under the Digital Pakistan Vision, the Ministry of Information Technology and Tele-communication issued the Draft National Artificial Intelligence Policy (the "Policy"). In order to accelerate socio-economic adoption, this policy looks towards adapting legal and regulatory frameworks needed to ensure safe and secure data-sharing mechanisms, considering international best practices.

In September 2024, the Regulation of Artificial Intelligence Act, 2024, was introduced in the Senate of Pakistan, aiming to regulate artificial intelligence (AI) in the country – though this is yet to be passed. The draft of this Act is presently under consideration by the Standing Committee on Information Technology and Telecommunication.

1.6 Data Breach Requirement

In the event of a personal data breach, where the breach is likely to result in any risk to the rights of the data subjects, the data controller must notify the Commission and the affected data subject without

undue delay and, where feasible, no later than 72 hours after becoming aware of the breach.

The data breach notification must include the following:

- a description of the nature of the personal data breach;
- the name and details of the data protection officer;
- the consequences of the personal data breach; and
- the measures adopted or suggested by the data controller to address the personal data breach.

In addition, data controllers need to maintain a record of any personal data breaches that have occurred.

As Pakistan does not yet have an operative data protection law in force, there is currently no active supervisory authority conducting investigations into personal data breaches. However, the proposed National Commission for Personal Data Protection would be empowered to investigate such breaches once established.

1.7 Regulators

The Draft Bill provides for the establishment of the National Commission for Personal Data Protection (NCPDP). The NCPDP shall be responsible for:

- protecting the interests of individuals;
- enforcing protection of personal data;
- preventing any misuse of personal data;
- promoting awareness of data protection; and
- addressing complaints.

1.8 Enforcement Proceedings and Fines

Administrative proceedings under the Draft Bill can be initiated with the filing of a complaint against any:

- violation of personal data protection rights;
- misconduct of any data controller or data processor;
- breach of a data subject's consent to process data; or
- breach of a data controller's obligations.

The complaint must be filed in a simple written format, and the complainant must certify that they have not already or concurrently filed any application, complaint or suit before any other forum or court.

An individual whose identity information has been obtained, possessed, distributed or used without authorisation may file a complaint with the Federal Investigation Agency (FIA). Where the victim seeks to block access to identifiable information or secure its destruction, they may approach the Pakistan Telecommunication Authority (PTA), established under the Pakistan Telecommunication (Re-Organization) Act 1996.

Any malpractice carried out by a bank with respect to the secrecy of customers' data may be challenged before the banking *muhtasib* (banking ombudsman).

Once an investigation is initiated and the relevant law is applied, administrative fines are imposed in accordance with the provisions of the respective laws that define the offence and prescribe the corresponding fines or penalties.

As of January 2026, there are no publicly reported cases of administrative fines having been issued in Pakistan specifically for breaches of individual privacy rights. The Draft Bill, however, provides for fines of up to USD2 million for unlawful processing of personal data.

1.9 Enforcement Trends

No enforcement trends have been recorded.

2. Privacy Litigation

2.1 Privacy Litigation Overview

The absence of a data protection law has resulted in a corresponding absence of dedicated privacy litigation in Pakistan.

2.2 Recent Case Law

There is no applicable information in this jurisdiction.

2.3 Collective Redress Mechanisms

The Draft Bill does not provide for any collective redress mechanism.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Currently, Pakistan does not have a specific, standalone regulation dedicated exclusively to governing the use of internet of things (IoT) services.

3.2 Interaction of Data Regulation and Data Protection

The interplay between these domains is rooted in the necessity to align data regulation frameworks with data protection principles rather than allowing them to conflict.

Regulatory bodies such as the PTA and the SBP monitor compliance with data regulations within their domains.

The NCPDP, once operational, will oversee compliance with the Draft Bill, impose penalties for violations and manage grievances.

3.3 Rights and Obligations Under Applicable Data Regulation

There is no applicable information in this jurisdiction.

3.4 Regulators and Enforcement

There is no applicable information in this jurisdiction.

4. Sectoral Topics

4.1 Use of Cookies

The Draft Bill does not specifically address requirements regarding the use of cookies; however, it has laid down the basic principles for processing, such as purpose specification, limitation, lawfulness, transparency, data retention, etc. These need to be followed by data controllers and processors while using cookies.

4.2 Personalised Advertising and Other Online Marketing Practices

The Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009, require all operators (holding a licence from the PTA) to establish a standard operating procedure (duly approved by the PTA) to control spamming.

Similarly, all operators are required to develop a standard operating procedure for controlling unsolicited calls. The operators are also required to establish a consolidated “Do Not Call Register” in connection with controlling unsolicited calls. The operators are further required to ensure registration of telemarketers.

The Draft Bill provides that data subjects must not be subjected to automated decision-making, including profiling that presents significant harm to data subjects.

4.3 Employment Privacy Law

Pakistan has no specific law concerning workplace privacy. The Draft Bill provides that sensitive personal data may be processed by a data controller for the purposes of exercising or performing any right or obligation conferred or imposed by law on the data controller in connection with employment.

The Public Interest Disclosures Act, 2017, governs the mechanism for public interest disclosures and protection of persons making such disclosures (related to the prevention of corruption in public sector organisations). Anonymous or pseudonymous disclosures are not considered under said Act. The identity of the complainant is to be protected unless required otherwise. The Act provides protection to the complainant against any victimisation on the ground that they made a disclosure. A complainant is considered victimised if they are:

- dismissed;
- suspended;
- denied promotion;
- demoted;
- made redundant;
- harassed;
- intimidated;

- threatened with any of the above matters; or
- subjected to discriminatory or other adverse measures by their employer or by a fellow employee.

Said Act also provides for due protection of the complainant, witness or any other person rendering assistance in an inquiry.

The Securities and Exchange Commission of Pakistan (SECP) has issued the Listed Companies (Code of Corporate Governance) Regulations, 2019 (the “Code”). The Code requires that listed companies’ boards of directors maintain a whistle-blowing policy, by establishing a mechanism to receive and handle complaints in a fair and transparent manner while providing protection to the complainant against victimisation. The Code requires that the chief executive officer of a listed company place “reports on/synopsis of issues and information pursued under the whistle-blowing policy, clearly disclosing how such matters were dealt with and finally resolved or cancelled”, before the board of directors or before the committee of the board of directors.

Matters pertaining to the role of labour organisations, e-discovery issues, use of digital loss-prevention technologies and scanning/blocking websites at a workplace are not dealt with under the Draft Bill or under any other law.

4.4 Data Protection in M&A

No regulatory framework is available governing data protection in M&A.

5. International Considerations

5.1 Restrictions on International Data Transfers

Under the Draft Bill, the transfer of personal data outside Pakistan is only permissible in the following cases:

- equivalent protection;
- explicit consent of the data subject; and
- under a framework to be devised by the NCPDP.

In the absence of an adequate data protection legal regime, the NCPDP may allow for the transfer of personal data outside Pakistan in the following cases:

- for a binding contract/agreement;
- with the explicit consent of the data subject provided it does not conflict with the public interest or national security of Pakistan;
- when international co-operation is required under relevant international obligations; and
- subject to any further conditions specified by the NCPDP.

It should be noted that critical personal data is not allowed to be transferred outside Pakistan.

Under the Draft Bill, the NCPDP is required to devise a mechanism for keeping some components of sensitive personal data within Pakistan (ie, data localisation).

The NCPDP shall also devise a mechanism for sharing sensitive personal data with the government of Pakistan, provided that the data relates to public order or national security and is required within the parameters of applicable law.

5.2 Government Notifications and Approvals

Under the Draft Bill, one of the permissible mode of cross-border transfer of personal data is a “mechanism to be devised by the NCPDP”. On establishment of the NCPDP, said mechanism may contain any approval requirements for all or any class of personal data.

5.3 Data Localisation Requirements

The Draft Bill provides that critical personal data must be kept within Pakistan.

5.4 Blocking Statutes

There are no blocking statutes related to data privacy or otherwise.

5.5 Recent Developments

No such developments have been noted.



Law and Practice

Contributed by:

Alex Saleh, Asad Ahmad, Jehan Saleh and Mounir Hany

GLA & Company

Contents

1. Legal and Regulatory Framework p.367

- 1.1 Overview of Data and Privacy-Related Laws p.367
- 1.2 Rights and Obligations p.368
- 1.3 Special Categories of Personal Data p.369
- 1.4 Processing of Personal Data for Research and Development Purposes p.369
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.370
- 1.6 Data Breach Requirement p.370
- 1.7 Regulators p.371
- 1.8 Enforcement Proceedings and Fines p.371
- 1.9 Enforcement Trends p.371

2. Privacy Litigation p.372

- 2.1 Privacy Litigation Overview p.372
- 2.2 Recent Case Law p.372
- 2.3 Collective Redress Mechanisms p.372

3. Requirements for the Protection and Processing of Non-Personal Data p.372

- 3.1 Objectives and Scope of Data Regulation p.372
- 3.2 Interaction of Data Regulation and Data Protection p.373
- 3.3 Rights and Obligations Under Applicable Data Regulation p.373
- 3.4 Regulators and Enforcement p.373

4. Sectoral Topics p.373

- 4.1 Use of Cookies p.373
- 4.2 Personalised Advertising and Other Online Marketing Practices p.374
- 4.3 Employment Privacy Law p.374
- 4.4 Data Protection in M&A p.374

5. International Considerations p.375

- 5.1 Restrictions on International Data Transfers p.375
- 5.2 Government Notifications and Approvals p.376
- 5.3 Data Localisation Requirements p.376
- 5.4 Blocking Statutes p.376
- 5.5 Recent Developments p.376

GLA & Company is the premier full-service regional law firm committed to delivering exceptional legal solutions across the Middle East and North Africa. With eight strategically located offices in seven key jurisdictions – UAE, KSA, Oman, Qatar, Kuwait, Bahrain and Egypt – the firm is positioned to serve its clients with unparalleled expertise and dedication. Founded

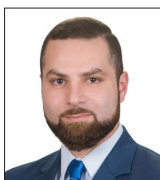
by a team of experienced legal professionals, GLA & Co has grown to encompass over 18 partners and more than 170 lawyers across the MENA region. Its diverse team is united by a shared commitment to excellence and a deep understanding of the unique legal landscapes of the jurisdictions it operates in.

Authors



Alex Saleh is the managing partner of GLA & Co and takes a leading regional role within the firm with respect to its Corporate & Commercial practice. With over 30 years of experience in both the GCC

markets as well as the US, he has accumulated sizeable expertise in the areas of banking and finance, mergers and acquisitions, capital market deals and infrastructure projects.



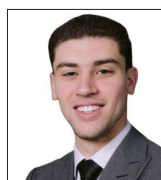
Asad Ahmad is a partner and head of the Antitrust & Competition practice at GLA & Co, leading the firm's regional practice across Kuwait, KSA, Qatar, UAE, Egypt and COMESA. He advises clients on merger control,

competition compliance and regulatory matters, securing major clearances and handling high-profile investigations. Asad also leads GLA & Co's Data Privacy team, guiding multinational clients on regulatory compliance and data protection strategies. A dedicated mentor and thought leader, he contributes to legal publications, conducts webinars and actively engages with competition regulators, reinforcing GLA & Co's reputation as a leader in antitrust and competition law.



Jehan Saleh is an associate attorney at GLA & Co. Her practice focuses primarily on corporate transactions and commercial advisory. A graduate of Wayne State Law School, Jehan has previously clerked for a judge in

the Wayne County Circuit Court in Michigan. Prior to joining the firm, Jehan was an associate attorney for a mid-sized law firm in the United States where she practised civil litigation. Jehan's Gulf experience includes working in the legal department for a large rideshare company in Dubai.



Mounir Hany is a corporate and commercial lawyer at GLA & Co with a practice spanning corporate governance, competition and trade remedies, and maritime commercial matters. He advises clients across

diverse sectors supporting complex commercial transactions and cross-border legal projects drafting complex transaction documents, including JVs, SPAs, SHAs, escrow agreements and SAFE notes.

GLA & Company

Alex Saleh
Managing Partner

Tel: Kuwait: +(965) 669 55516

UAE: +(971) 54 997 4040

Email: alex.saleh@glaco.com

Web: glaco.com/attorneys/alex-saleh/



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Qatar introduced Law No 13 of 2016 on Protecting Personal Data Privacy (the “Personal Data Privacy Protection Law”, or PDPPL), which took effect in 2017.

The PDPPL applies to personal data when it is electronically processed, or obtained, gathered or extracted in preparation for electronic processing, or processed via a combination of electronic and traditional processing. The PDPPL aligns with, but is not as stringent as, the universal data protection principles that were established as the core of the European Union’s General Data Protection Regulation (GDPR). The PDPPL explicitly excludes personal data processed by individuals within a private or family scope.

The PDPPL establishes key definitions central to its application: “Personal Data” is defined as data of an individual whose identity is defined or can be reasonably defined whether through such personal data or through the combination of such data with any other data. “Personal Data Processing” encompasses a broad range of activities including gathering, receipt, registration, organisation, storage, preparation, modification, retrieval, usage, disclosure, publication, transfer, withholding, destruction, erasure and cancellation. “Cross-Border Data Flow” means accessing, watching, retrieving, using or storing personal data without restrictions of the State’s borders.

The Compliance and Data Protection Department (CDPD) attached to the Ministry of Communications and Information Technology (MCIT) (previously known as the Ministry of Transport and Communications) published guidelines concerning the PDPPL (the “PDPPL Guidelines”) in 2021, with the aim of providing a framework for data protection in Qatar. The National Cyber Security Agency (NCSA) has also issued the Guidelines for Secure Adoption and Usage of Artificial Intelligence, which provide guidance on how to securely deploy AI systems while complying with PDPPL requirements.

The PDPPL was enacted after perusal of the Constitution and operates alongside several related laws.

The preamble to the PDPPL explicitly references the following foundational legislation:

- the Telecommunications Law promulgated by Decree Law No 34 of 2006;
- the Electronic Transactions and Commerce Law promulgated by Decree Law No 16 of 2010;
- Law No 2 of 2011 on Official Statistics (as amended by Law No 4 of 2015); and
- the Cybercrimes Combating Law promulgated by Law No 14 of 2014.

Qatar’s data protection and privacy regime is also composed of provisions relating to penalties in other laws, such as:

- the Penal Code promulgated by Law No 11 of 2004;
- the Trade Secrets Law promulgated by Law No 5 of 2005;
- the Qatar Constitution;
- the Labour Law promulgated by Law No 14 of 2004; and
- the Qatar Banking Regulations issued by the Qatar Central Bank, governed by Law No 13 of 2012.

While these laws supplement data protection and privacy laws in Qatar, the PDPPL is the detailed framework for the protection of personal data in Qatar.

Qatar operates a dual legal system for data protection. In addition to the “mainland” or “State” system and the PDPPL described above, there is a separate legal data privacy protection regime in the Qatar Financial Centre (QFC). The QFC is a business and financial hub in Qatar that provides a legal, regulatory and tax environment distinct from “mainland Qatar”. It operates under its own legal framework and has its own independent judiciary. The key data protection legislation for the QFC is the QFC Data Protection Regulations 2021 (the “QFC Regulations”).

The Data Protection Office (DPO) is an independent institution of the QFC. It is charged with administering the QFC Regulations and all aspects of data protection within the QFC. Entities operating within the QFC are subject to the QFC Regulations rather than the

PDPPL, creating a distinct regulatory environment for financial services and related businesses.

Extraterritorial Reach

The PDPPL does not contain explicit provisions regarding extraterritorial application. Unlike the EU's GDPR, which expressly extends to controllers and processors outside the EU that offer goods or services to, or monitor the behaviour of, EU residents, the PDPPL is primarily focused on processing activities within Qatar. However, the law's provisions regarding Cross-Border Data Flow indicate that controllers should not take any decision or measure that may limit cross-border data flow, unless the processing of such data is in breach of the law or may cause serious damage to personal data or to the individual's privacy.

Governmental exemptions under Article 18 of the PDPPL permit certain processing activities without compliance with specific provisions for purposes of national security, international relations, economic or financial interests of the State, and prevention or investigation of criminal offences.

Interplay With Cyber and AI Laws

The PDPPL operates in conjunction with the Cybercrimes Combating Law. The NCSA is responsible for enforcement of both cybersecurity and data protection matters, and all data breaches should be reported to the NCSA.

The NCSA's Guidelines for Secure Adoption and Usage of Artificial Intelligence address critical risks such as privacy violations, AI bias, security vulnerabilities and compliance challenges, particularly in sectors where AI processes personal data (such as finance, healthcare and law enforcement). AI systems must comply with PDPPL requirements for data minimisation, purpose limitation and lawful processing. AI models must incorporate auditability, traceability and documentation requirements. Additionally, the Qatar Central Bank has issued guidelines to ensure the ethical use of AI in the financial sector, mirroring PDPPL safeguards regarding data collection, processing purposes, transparency and explicit consent requirements.

1.2 Rights and Obligations

Personal data must be processed lawfully, fairly and transparently, and only for specific, explicit and legitimate purposes. Processing must be limited to what is adequate, relevant and proportionate to the stated purpose, and data must be accurate, complete and kept up to date.

As a general rule, processing requires the prior consent of the data subject, which must be informed and specific.

Personal data may not be retained for longer than necessary to achieve the purpose of processing, subject to any mandatory legal retention obligations. Data controllers are required to implement appropriate technical and organisational security measures to protect personal data against unauthorised access, disclosure, alteration, loss or destruction. These security and confidentiality obligations are reinforced under the Telecommunications Law and the Cybercrimes Combating Law.

The processing of sensitive personal data, such as health-related information, is subject to enhanced safeguards and typically requires explicit consent or express legal authorisation.

The cross-border transfer of personal data outside Qatar is restricted unless the recipient jurisdiction ensures an adequate level of protection, approval is obtained from the competent authority, or a statutory exception applies.

Data Subject Rights

Under the PDPPL, data subjects are afforded a number of core rights, including:

- the right to be informed of the collection and processing of their personal data;
- the right of access to personal data held about them;
- the right to rectification of inaccurate or incomplete personal data;
- the right to erasure of personal data where it is no longer necessary or is unlawfully processed, subject to legal retention requirements;

- the right to object to certain types of processing; and
- the right to withdraw consent at any time where processing is based on consent.

In addition, the Telecommunications Law protects the confidentiality of communications and related data, subject only to lawful disclosure or interception.

Organisations operating in Qatar and processing personal data should focus on the following core compliance measures:

- *Identify and document processing activities:* Map personal data flows, purposes of processing, categories of data subjects, and any third-party disclosures.
- *Establish a lawful basis for processing:* Ensure that each processing activity is supported by valid consent or a recognised statutory exemption.
- *Implement transparency measures:* Prepare and maintain clear privacy notices informing data subjects of how their data is processed.
- *Put in place data security controls:* Adopt appropriate technical and organisational safeguards proportionate to the nature and sensitivity of the data.
- *Manage data subject rights:* Implement procedures to receive, assess and respond to access, rectification, erasure and objection requests.
- *Control data retention:* Define and apply retention periods and ensure secure deletion once data is no longer required.
- *Assess cross-border transfers:* Review any transfers outside Qatar and ensure that legal requirements and approvals are met.
- *Prepare for incidents and enforcement risk:* Establish internal escalation and response procedures for data breaches and cyber incidents.

1.3 Special Categories of Personal Data

Under Qatari law, special categories of personal data – also referred to as sensitive personal data – include information relating to a person’s ethnic origin or race, physical or mental health, religious beliefs, relationships or marital status, criminal records and children. In the QFC, this definition additionally covers biometric data, genetic data and data relating to criminal convictions.

Processing of such data is generally prohibited unless prior approval is obtained from the MCIT or, in the QFC, a specific written permit from the Data Protection Officer (DPO). To obtain this permit, the data controller must provide details of the processing, its purpose, the categories of data subjects affected, any intended recipients, cross-border transfers, and the safeguards implemented to ensure security.

Sensitive personal data must be processed with explicit consent where no statutory exception applies, and organisations must implement enhanced security and confidentiality measures. The PDPPL and related regulations also require purpose limitation, data minimisation, accuracy, and limited retention of such data.

Processing data relating to minors requires additional care, typically involving parental or guardian consent, and full transparency regarding the processing purpose and safeguards.

Processing data relating to criminal convictions or offences is strictly controlled, allowed only under statutory authority, under legal requirements or with explicit consent, and subject to strong safeguards to prevent unauthorised access or disclosure.

In all cases, the processing of sensitive data carries heightened procedural and security obligations, and non-compliance may result in administrative, civil or criminal liability.

1.4 Processing of Personal Data for Research and Development Purposes

Under the PDPPL, companies providing products or services used by healthcare providers may process personal data, including patient data, only where such processing is based on the data subject’s consent or is necessary to achieve a lawful purpose (Article 4). The PDPPL does not expressly regulate or define “anonymisation”. However, to the extent that data is processed in a manner that no longer allows identification of an individual, such data would fall outside the scope of the PDPPL.

Where patient data constitutes personal data of a special nature (including health data), processing – including for product development or scientific research

– requires prior permission from the competent authority, and may be subject to additional safeguards (Article 16). The PDPPL provides a limited exemption permitting processing for scientific research conducted in the public interest, subject to the conditions and controls set out in the Law (Article 19).

Qatar has not enacted legislation equivalent to the European Health Data Space Regulation, and there is no specific health-data governance framework comparable to the EU regime. Accordingly, the European Health Data Space Regulation has no direct legal impact in Qatar, and life sciences companies operating in Qatar must comply with the PDPPL rather than EU-style secondary use or data-sharing obligations.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Under the PDPPL, the use of personal data in AI systems must comply with the same personal data protection obligations that apply to any processing of personal data: lawful purpose, transparency, consent or necessity, data minimisation, and appropriate safeguards against unauthorised access or misuse. These general principles are the core legal requirements for AI-related data processing under Qatari law.

Qatar has not yet enacted a standalone AI data protection law, but there are emerging policy and guidance developments that shape how AI systems handling personal data should operate:

- The PDPPL's framework itself requires controllers to process personal data only for lawful and specified purposes and to respect data subject rights, which by extension applies to AI systems that use personal data.
- Qatar's national AI guidelines and policies (eg, the AI Guidelines for Developers issued by the MCIT) explicitly emphasise that organisations must respect personal data protection and privacy obligations under the PDPPL when designing or deploying AI systems. These guidelines reinforce the need to ensure that personal data is not exposed or published without lawful basis and that users can flag privacy issues.
- Sector-specific guidance, such as financial sector AI guidelines, mirrors PDPPL principles by

requiring that AI systems only collect and process personal data necessary for their function and that individuals are informed about how their data is processed by AI.

- Broader national initiatives (including Qatar's regulatory landscape for AI) are moving towards comprehensive governance frameworks, with AI ethics and data protection principles layered on top of the PDPPL for responsible AI adoption across sectors.

There is no risk-based classification, prohibited high-risk categories or binding AI regulation akin to the EU's AI Act in Qatar's PDPPL. Instead, all AI-related processing of personal data must simply align with the PDPPL's core standards of lawful processing, transparency, purpose limitation and safeguards, with any higher-risk processing (such as sensitive personal data) requiring prior authority approval per Article 16 of the PDPPL.

1.6 Data Breach Requirement

A personal data breach under Qatari law occurs when there is a breach of security leading to the unlawful or accidental alteration, destruction, loss or unauthorised disclosure of or access to personal data. Breaches may be deliberate or accidental, and can affect both individuals and organisations.

Examples of breaches include:

- theft or loss of IT equipment containing personal or sensitive data;
- unauthorised access to customer or employee data;
- leaving confidential files unattended;
- inadequate disposal of documents containing personal data; and
- unauthorised disclosure or use of client data for personal gain.

Requirements and actions for organisations:

- *Immediate containment and assessment:* Identify the nature, scope and potential impact of the breach.
- *Notification to the competent authority:* Under the PDPPL, report serious breaches to the MCIT, or, in the QFC, to the DPO.

- *Notification to affected data subjects:* Notify affected data subjects where the breach is likely to result in significant risk to the rights and freedoms of data subjects.
- *Documentation and record-keeping:* Maintain records of the breach, causes and corrective measures taken.
- *Mitigation and corrective measures:* Implement technical and organisational safeguards to prevent further breaches, including access controls, encryption, secure disposal and staff training.
- *Post-incident review:* Update policies and procedures to prevent recurrence.

Consequences and Regulatory Oversight

Breaches can result in financial loss, reputational damage, legal liability or disruption to operations.

Under the PDPPL and Cybercrimes Combating Law, the MCIT or DPO may investigate breaches, impose administrative fines or, in cases of deliberate misconduct, initiate criminal proceedings.

1.7 Regulators

The CDPD at the MCIT is the key regulator in Qatar, and the NCSA is the competent department for administration and enforcement of the PDPPL. It is the key authority for conducting investigations regarding cybersecurity issues, implementing and examining issues related to national cyber-risks, and conducting fieldwork solidifying resilience against cybercrimes and crises. All data breaches should be reported to the NCSA.

In the QFC, the DPO is concerned with the data protection framework. It is the institution charged with providing guidance on all data protection matters or complaints related to the QFC Regulations. The DPO is concerned with the protection of the rights of individuals and ensuring implementation of protection measures for all QFC entities, firms or future investors.

1.8 Enforcement Proceedings and Fines

The enforcement process is usually triggered by a complaint filed before the NCSA, which is the competent authority in the State of Qatar. The NCSA will commence an investigation process in order to verify the veracity of the complaint; thereafter, if warranted,

it will issue a judicial order binding the controller or processor in line with its powers under the law.

The competent department, as listed in the PDPPL, will issue a rectification decision, ordering the violating entity to rectify the violation within a fixed period, as per Article 26 of the PDPPL. Previously it was understood that the competent department was the MCIT; however, recently the NCSA clarified that this department was not yet designated. The controller or processor has the right to file a “grievance” against such order to the relevant minister within 60 days from the date of notification. The decision issued by the minister related to such grievance shall be deemed final, according to Article 26 of the PDPPL. According to Article 29 of the PDPPL, the judicial officers and/or law enforcement officers designated by the NCSA have the power to document any offences and to seize any related materials, equipment or evidence in accordance with applicable procedure related to violations of the provisions of the law.

Furthermore, in the QFC, if the DPO determines a contravention or violation of the law by any data controller, a direction would be issued to the data controller to undertake the following, in compliance with Article 22 of the QFC Regulations:

- to act or omit from performing any step; and
- to refrain from processing any personal data specified in the direction or to refrain from processing personal data for a purpose or in a manner specified in the direction.

1.9 Enforcement Trends

In the past 24 months in Qatar, there have been no widely reported, publicly available enforcement actions specifically under the PDPPL. Data protection enforcement in Qatar tends to be handled administratively by the competent authority rather than through public court judgments, and details of specific sanctions or enforcement decisions are generally not published publicly.

Practical takeaways for organisations:

- Treat PDPPL compliance as a proactive regulatory requirement, not a reactive one, even in the absence of public enforcement actions.
- Ensure lawful bases for processing, implement appropriate security safeguards and maintain documentation of processing activities.
- Establish internal mechanisms to handle data subject rights and potential complaints to the competent authority.
- Recognise that enforcement may occur administratively, and organisations should be prepared to respond to audits, investigations or directions from the authority.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Privacy and data-related litigation in Qatar remains limited and is not public. There is no publicly available body of case law showing a discernible trend in privacy or data protection disputes before the courts in the past 24 months. As a result, there is no clear pattern as to claimant types, causes of action, or remedies specifically grounded in data protection or privacy breaches. While the PDPPL provides a statutory framework for personal data protection and contemplates sanctions for violations, reported judicial decisions applying these provisions in civil litigation are scarce, and privacy litigation can be considered to be at an early stage in the jurisdiction.

2.2 Recent Case Law

There are no publicly reported court decisions in Qatar that have materially shaped a framework for privacy or data protection litigation comparable to landmark case law in other jurisdictions. In practice, the interpretation and application of data protection obligations are primarily driven by the statutory provisions of the PDPPL and guidance issued by the competent authority, rather than by judicial precedent. Consequently, there are no established judicial standards equivalent to those developed through EU-level case law.

2.3 Collective Redress Mechanisms

Under the PDPPL, there is no collective or representative redress mechanism for privacy or data protection

claims. The PDPPL provides for an individual complaint mechanism only, whereby an individual may file a complaint with the competent department in the event of a violation of the Law, and the competent department may investigate and issue a binding decision requiring the controller or processor to rectify the breach (Article 26). The PDPPL does not contemplate group actions, representative claims or collective proceedings, and there have been no legislative developments introducing collective redress frameworks for data protection matters in Qatar.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Under Qatari law, there is no specific legal regime governing non-personal data akin to the EU Data Act or comprehensive cross-sector data-sharing frameworks for the Internet of Things (IoT), cloud computing, big data or similar services.

At present, there is no dedicated law, case law or published guidance in Qatar that establishes a cross-sector non-personal data governance framework, data access sharing rights for non-personal data holders and users, or obligations similar to the EU Data Act. The available legal instruments focus on the protection of personal data and related processing obligations.

Some policy documents such as government data management or data-sharing policies (eg, initiatives for inter-agency data exchange) exist in the public sector and envisage structured sharing of non-personal data among government entities under agreed standards and conditions (eg, through a central data exchange platform), but these are policy/operational instruments rather than standalone statutory laws and do not create statutory rights analogous to EU data governance laws.

Qatar has not yet enacted legislation similar to the EU Data Act, and there is no public indication of an imminent data governance law specifically for non-personal data comparable to the EU framework.

In practice therefore, organisations in Qatar that handle non-personal data rely on sector-specific rules and contracts (eg, cloud service agreements, telecom or banking security standards) and any applicable government data policies when sharing or using such data, but there is no overarching legal regime specifically governing non-personal data at present.

3.2 Interaction of Data Regulation and Data Protection

The PDPPL is closely linked to other Qatari laws regulating cybersecurity and digital transactions. The NCSA enforces cybersecurity laws and plays a role in ensuring personal data protection in AI applications and IoT services. The Telecommunications Law and Cybercrime Law impose additional restrictions on electronic data processing and cybersecurity threats.

3.3 Rights and Obligations Under Applicable Data Regulation

Under the PDPPL, the statutory rights and obligations apply only to personal data. The PDPPL does not regulate non-personal data, and therefore does not establish rights or obligations relating to the use, sharing, portability, interoperability, switching, termination, FRAND access or mandatory data sharing in respect of non-personal data.

In relation to personal data, the PDPPL grants individuals core rights, including the right to be informed of processing and its purposes, the right to access and obtain a copy of their personal data, the right to request correction of inaccurate data, the right to object to processing where it is not necessary for a lawful purpose, the right to withdraw consent, and the right to request erasure where the purpose for processing has ceased or no longer exists. The PDPPL does not provide for data portability, interoperability, switching rights, FRAND access, or mandatory data sharing between organisations.

From an obligations perspective, controllers must ensure that personal data is processed for a lawful purpose, based on either consent or necessity, and in a manner that is fair, proportionate, and limited to what is required. Controllers must comply with transparency requirements, maintain data accuracy and relevance, avoid excessive retention, and implement

appropriate administrative, technical and financial safeguards to protect personal data. Controllers are also required to manage and report serious personal data breaches and to obtain prior permission from the competent authority where processing involves personal data of a special nature.

In addition to the PDPPL itself, the competent authority has issued non-binding implementation guidelines to support compliance. The PDPPL Guidelines provide practical guidance, templates and checklists to assist organisations in operationalising PDPPL requirements, including governance measures, security controls, transparency practices and handling of data subject rights. While not legally binding, they are relevant in demonstrating good-faith compliance with the PDPPL.

Accordingly, key action items for organisations include identifying whether data processed constitutes personal data, defining and documenting lawful purposes, implementing consent and transparency mechanisms, putting in place appropriate security and governance measures, establishing procedures to respond to data subject rights requests, limiting retention periods, and seeking prior approval where required for processing sensitive personal data.

3.4 Regulators and Enforcement

See 1.7 Regulators.

4. Sectoral Topics

4.1 Use of Cookies

According to the PDPPL Guidelines, controllers may use “cookies” on an individual’s web browser to target direct advertisement messages towards the individual. Such cookies should be deployed only after the individual has “opted in” – ie, has clicked “accept” to allow such direct marketing cookies to be deployed on the individual’s browser.

Controllers may collect individuals’ email addresses on a web page of the controller’s website. The controller must make it clear, on the web page, that if the individual provides their email address in that instance they are providing their consent towards receiving

direct marketing emails until they withdraw their consent.

4.2 Personalised Advertising and Other Online Marketing Practices

Article 22 of the PDPPL and the PDPPL Guidelines explicitly prohibit unsolicited direct marketing or marketing communications. Prior consent to send electronic marketing communications is required, including by wired or wireless communication. The PDPPL recognises that the consent must be explicit and unambiguous. It is worth noting that implied consent is not recognised under the PDPPL and will mostly be deemed as invalidly taken.

The following information must be included in all electronically shared communications:

- the identity of the sender;
- an indication that the message is sent for the purpose of direct marketing;
- a reachable and searchable address; and
- a communication platform enabling the customer to request withdrawal of its consent and request the immediate cessation of all upcoming communications.

4.3 Employment Privacy Law

Currently, there is no freedom of information legislation in the State of Qatar – a step being discussed by most practitioners. In the same vein, the focus is on organisations and employers, which would need to display that permission was duly received from employees for the assessment and collection of their personal sensitive and classified data.

According to the PDPPL, workplace privacy rules strictly provide for a solid framework for protecting an employee's privacy. Thus, organisations must provide proof or evidence that they have a permitted reason to process their employees' personal data (SISCO systems, telephone or PC monitoring, GPS). Employers will also need to conduct data protection impact assessments when processing employees' personal data, as this is considered by the CDPD as an example of processing that "may cause serious damage".

In parallel, the Labour Law requires employers to maintain employee files and registers containing personal and employment-related information, including identification details, wages, leave records, disciplinary sanctions and termination information, and to retain such records for prescribed periods. These obligations do not override the PDPPL, and employers must ensure that the collection, storage and retention of employment records under the Labour Law are carried out in compliance with the PDPPL's privacy and data protection requirements.

On 24 May 2021, the Ministry of Administrative Development, Labour and Social Affairs (MADLSA) launched the first phase of the Unified Platform for Complaints and Whistle-blowers. Through this electronic platform, citizens, expatriates and establishments can file a complaint against entities subject to the provisions of Qatar Labour Law promulgated by Law No 14 of 2004 and the Domestic Workers Law promulgated by Law No 15 of 2017, or against entities with business regulated by the MADLSA.

4.4 Data Protection in M&A

The PDPPL applies to the processing of personal data where such data is electronically processed, prepared for electronic processing, or processed using a combination of electronic and traditional means. It does not regulate non-personal data.

During due diligence, the disclosure or access to personal data constitutes personal data processing, including disclosure and transfer. Accordingly:

- Personal data may only be processed for a **lawful purpose**, either based on the data subject's consent or where processing is necessary to achieve a lawful purpose of the controller or recipient (Article 4).
- Any disclosure of personal data must be **consistent with the lawful purposes** for which the data was collected (Article 12).
- Controllers and processors must implement **appropriate administrative, technical and financial safeguards** to protect personal data against unauthorised access, disclosure or misuse (Articles 8, 11 and 13).

- Personal data disclosed during due diligence must be **adequate, relevant and not excessive**, and must not be retained for longer than necessary for the relevant purpose (Article 10).

The PDPPL does not contain specific provisions tailored to M&A due diligence; compliance is assessed under the general processing obligations.

The PDPPL does not expressly regulate “change of control”. However, a change in ownership or control that results in a new entity determining the purposes and means of processing may constitute a change in the controller.

In such cases:

- Personal data may continue to be processed only for **lawful purposes** consistent with the PDPPL (Article 4).
- The controller must ensure that individuals are **informed of the identity of the controller and the purposes of processing**, and any material change to processing activities must be consistent with the information provided to individuals (Article 9).
- Any transfer of personal data to a new controller must comply with the **disclosure and safeguarding requirements** of the PDPPL (Articles 12 and 13).

The PDPPL requires controllers, prior to processing personal data, to inform individuals of:

- the controller’s identity;
- the lawful purposes of the processing; and
- a description of the processing activities and levels of disclosure (Article 9).

While the PDPPL does not mandate transaction-specific notifications, any post-transaction change that affects these elements must remain compliant with the transparency requirements under Article 9.

Please note that if the transaction involves personal data of a special nature (eg, health data, children’s data, religious beliefs, criminal data), such data may only be processed – including being disclosed or transferred in the context of an M&A or asset deal –

with prior permission from the competent authority and subject to any additional safeguards imposed.

5. International Considerations

5.1 Restrictions on International Data Transfers

“Cross-Border Data Flow” is defined under the PDPPL as accessing, viewing, retrieving, using or storing personal data without border constraints. The PDPPL provides that data controllers should not take measures or adopt procedures that may restrict or prevent Cross-Border Data Flow, unless processing such data would violate the provisions of the PDPPL or cause gross damage to the data subject.

More specifically, the PDPPL reserves the right for governmental bodies to decide that certain obligations under the Law (including those relating to Cross-Border Data Flow) do not apply to certain categories of data they process, based on the following grounds:

- national security;
- international relations;
- the economic or financial interests of the State; or
- the prevention or investigation of criminal offences.

A Cross-Border Data Flow may occur where the data exporter is:

- performing a task pertaining to the public good;
- executing a court order;
- protecting the vital interests of the individual;
- meeting the objectives of scientific research; or
- collecting information to investigate a crime when requested by officials.

The PDPPL does not prescribe specific transfer mechanisms (such as adequacy determinations, standard contractual clauses or transfer impact assessments) for lawful Cross-Border Data Flow. Compliance is assessed by reference to adherence to the PDPPL’s general processing principles and safeguards.

In addition, personal data of a special nature may only be processed, including through cross-border trans-

fer, with prior permission from the competent authority and subject to any additional safeguards imposed.

Qatar is yet to enter into mutual legal assistance treaties or bilateral treaties to ensure appropriate involvement of the authorities in countries where the data is stored. The PDPPL does not condition the legality of Cross-Border Data Flow on the existence of such treaties.

5.2 Government Notifications and Approvals

Situations where a notification or approval would most likely be required to transfer data internationally or to carry out cross-border transfer would be in the context of QFC transfers. In principle, the QFC does not maintain a list of “adequate” jurisdictions. However, in certain circumstances, when the recipient in a country is not deemed to have an adequate level of protection for personal data, this would essentially require obtaining a permit for the transfer and the data controller would apply certain safeguards in accordance with Article 10 (1)(a) of the QFC Regulations.

5.3 Data Localisation Requirements

There is no general data localisation requirement or prior approval requirement for cross-border transfers under the PDPPL, except in the case of personal data of a special nature, which requires prior permission from the competent authority (Article 16).

From an operational perspective, according to the Communications Regulatory Authority (Qatar’s telecommunications and digital services regulator), it is no longer necessary for data to be stored “on premises” or “locally”. Instead, organisations should implement security measures such as encryption, anonymisation and aggregation at predefined secure hubs (regions/availability zones), which are more efficient than localisation.

The Cloud Policy Framework (CPF) issued in June 2022 sets the roadmap for more concrete considerations relating to the above-mentioned circumstances and operations. According to the CPF, data residency shall no longer be a requirement as data classification schemes, security and encryption technologies now secure a high level of protection controls.

These are newly discussed concepts, but it is expected that data localisation may be required for extremely sensitive data only, and that this would constitute one of the limitations to an organisation collecting or transferring data in connection with foreign government data requests or foreign litigation proceedings.

5.4 Blocking Statutes

Pursuant to Article 15 (3) of the QFC Regulations, a data subject has the right to require and obtain from the data controller – upon request, at reasonable intervals and without excessive delay or expense, as appropriate – the rectification, erasure or blocking of personal data, the processing of which does not comply with the law.

5.5 Recent Developments

Under the PDPPL, cross-border transfers of personal data are permitted in principle.

The PDPPL expressly recognises “Cross-Border Data Flow” and provides that a controller may not restrict the transfer of personal data outside the State unless the processing violates the Law or may cause serious damage to the personal data or the individual’s privacy (Article 15).

Accordingly, international transfers are allowed provided that:

- the processing serves a lawful purpose;
- the controller complies with the PDPPL’s general data protection obligations (including security safeguards and transparency); and
- the transfer does not result in serious harm to personal data or individual privacy.

There have been no recent developments in the regulation of the international transfer of personal data. Under the law, it is not restricted. However, given that neighbouring countries have enacted amendments to supplement their own data protection laws, Qatar may follow suit by introducing updates to the PDPPL to align with regional and global standards.

SAUDI ARABIA

Law and Practice

Contributed by:

Alex Saleh, Asad Ahmad, Shahad Alhumaidani and Omar Halbouni

GLA & Company



Contents

1. Legal and Regulatory Framework p.379

- 1.1 Overview of Data and Privacy-Related Laws p.379
- 1.2 Rights and Obligations p.380
- 1.3 Special Categories of Personal Data p.380
- 1.4 Processing of Personal Data for Research and Development Purposes p.381
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.381
- 1.6 Data Breach Requirement p.382
- 1.7 Regulators p.382
- 1.8 Enforcement Proceedings and Fines p.383
- 1.9 Enforcement Trends p.383

2. Privacy Litigation p.383

- 2.1 Privacy Litigation Overview p.383
- 2.2 Recent Case Law p.384
- 2.3 Collective Redress Mechanisms p.384

3. Requirements for the Protection and Processing of Non-Personal Data p.385

- 3.1 Objectives and Scope of Data Regulation p.385
- 3.2 Interaction of Data Regulation and Data Protection p.385
- 3.3 Rights and Obligations Under Applicable Data Regulation p.386
- 3.4 Regulators and Enforcement p.388

4. Sectoral Topics p.389

- 4.1 Use of Cookies p.389
- 4.2 Personalised Advertising and Other Online Marketing Practices p.389
- 4.3 Employment Privacy Law p.389
- 4.4 Data Protection in M&A p.390

5. International Considerations p.390

- 5.1 Restrictions on International Data Transfers p.390
- 5.2 Government Notifications and Approvals p.391
- 5.3 Data Localisation Requirements p.392
- 5.4 Blocking Statutes p.392
- 5.5 Recent Developments p.393

GLA & Company is the premier full-service regional law firm committed to delivering exceptional legal solutions across the Middle East and North Africa. With eight strategically located offices in seven key jurisdictions – UAE, KSA, Oman, Qatar, Kuwait, Bahrain and Egypt – the firm is positioned to serve its clients with unparalleled expertise and dedication. Founded

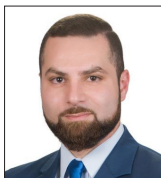
by a team of experienced legal professionals, GLA & Co has grown to encompass over 18 partners and more than 170 lawyers across the MENA region. Its diverse team is united by a shared commitment to excellence and a deep understanding of the unique legal landscapes of the jurisdictions it operates in.

Authors



Alex Saleh is the managing partner of GLA & Co and takes a leading regional role within the firm with respect to its Corporate & Commercial practice. With over 30

years of experience in both the GCC markets as well as the US, he has accumulated sizeable expertise in the areas of banking and finance, mergers and acquisitions, capital market deals and infrastructure projects.



Asad Ahmad is the legal director and head of the Antitrust & Competition practice at GLA & Co, leading the firm's regional practice across Kuwait, KSA, Qatar, UAE, Egypt and COMESA. He advises clients on

merger control, competition compliance and regulatory matters, securing major clearances and handling high-profile investigations. Asad also leads GLA & Co's Data Privacy team, guiding multinational clients on regulatory compliance and data protection strategies. A dedicated mentor and thought leader, he contributes to legal publications, conducts webinars and actively engages with competition regulators, reinforcing GLA & Co's reputation as a leader in antitrust and competition law.



Shahad Alhumaidani is an associate in GLA & Co's Riyadh office. Shahad holds experience working in both the governmental and private sectors in KSA and has the experience to advise on capital markets, corporate and commercial transactional and advisory matters including due diligence exercises, corporate governance, and mergers and acquisitions.



Omar Halbouni is an associate at GLA & Co, where he works closely with the firm's GCC-focused M&A, Private Equity, Capital Markets and Finance teams. He has advised both private and public companies, ranging from early-stage start-ups to Fortune 500 corporations, as well as royal family offices across the GCC. Prior to joining the firm, Omar gained valuable experience practising at an international law firm in North America.

GLA & Company

Alex Saleh
Managing Partner

Tel: Kuwait: +(965) 669 55516

UAE: +(971) 54 997 4040

Email: alex.saleh@glaco.com

Web: glaco.com/attorneys/alex-saleh/



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Data protection and privacy issues in the Kingdom of Saudi Arabia (KSA) are governed by a robust set of laws, regulations, policies, procedures, standards and guidelines.

The most notable of these laws is the Personal Data Protection Law of 16 September 2021, issued by Royal Decree M/19, and its amendments (together with the Implementing Regulations, the PDPL) came into force on 14 September 2023.

Other significant laws and regulations relating to the protection and privacy of data in KSA include, among others:

- Telecommunications and Information Technology Law no. M/160 of 2022 (the “TCIT Law”);
- Electronic Transactions Law no. M/18 of 2007 (the “ET Law”);
- Anti-Cyber Crime Law no. M/17 of 2007 (the “ACC Law”); and
- Electronic Commerce Law no. M/126 of 2019 (the “EC Law”).

Also, in August and September 2024, the Saudi Data & AI Authority (SDAIA) issued several new regulations to enhance and streamline the data privacy framework in KSA. These regulations are:

- regulation on personal data transfer outside KSA;
- rules for appointing personal data protection officer;
- data sharing policy;
- elaboration and developing privacy policy guidelines;
- minimum personal data determination guidelines;
- guidelines for binding common rules BCR for personal data transfer;
- standard contractual clauses for personal data transfer;
- personal data destruction, anonymisation and pseudonymisation guidelines;
- personal data disclosure cases guidelines;

- personal data processing activities records guidelines; and
- personal data breach incidents procedural guide.

The PDPL covers processing of personal data that (i) takes place in KSA or (ii) relates to individuals residing in KSA, by any means, by any party outside KSA. The TCIT Law covers communication services and protection of client and customer data and privacy. The ET Law covers electronic transactions, creating and keeping electronic records, electronic signatures and electronic authentication certificates. The ACC Law addresses cybersecurity crimes and their punishment. The EC Law covers the usage of customers’ data in electronic commerce transactions.

The policies, procedures, standards and guidelines are vast; however, those that are most relevant to data protection and privacy are:

- general principles for protecting users’ personal data privacy;
- procedures for launching services or products based on a customer’s personal data or regarding the sharing of personal data;
- national data governance policies;
- data management and personal data protection standards;
- general standards for personal data transfer beyond the geographical limits of KSA;
- children and incompetents’ privacy protection policy; and
- guidelines and specifications on data management governance and personal data security.

In KSA, the PDPL provides the baseline legal regime for any processing of personal data, while SDAIA’s National Data Management Office (NDMO) instruments govern government and non-personal data (including classification, sharing and de-identification standards), so mixed datasets are handled by applying the PDPL to the personal elements and NDMO governance to the rest, with the PDPL still attaching if re-identification is reasonably possible.

The PDPL’s security, breach notification and processor oversight duties operate alongside prescriptive cybersecurity controls from the National Cybersecu-

rity Authority's (NCA) Essential Cybersecurity Controls and sectoral frameworks (eg, the Saudi Central Bank (SAMA) for finance and the Communications, Space and Technology Commission (CST) for telecom/cloud).

The Anti-Cyber Crime Law adds criminal penalties for unlawful access, interception or misuse, meaning a single incident can trigger PDPL compliance, sectoral supervisory action and criminal exposure.

For AI, SDAIA's national AI strategy and ethics principles guide responsible development, but the PDPL governs whenever AI systems train (by feeding data), tune (by adjusting model parameters) or infer (by using the model) from personal data (lawful basis, transparency, minimisation, data protection impact assessments (DPIAs) for high-risk uses, heightened safeguards for sensitive data), while robust NDMO-aligned de-identification is required to move processing outside the PDPL, and cross-border PDPL transfer conditions and any localisation mandates under NDMO/CST/SAMA must be respected for cloud and AI pipelines, with organisations generally applying the strictest applicable rule across these overlapping frameworks.

1.2 Rights and Obligations

Under the PDPL, personal data must be processed lawfully, fairly and transparently for specified purposes, limited to what is necessary, accurate, retained only as required, and protected by appropriate technical and organisational measures. Controllers are accountable through governance arrangements, records of processing, and oversight of processors.

Sensitive personal data is subject to heightened safeguards and, in some cases, additional conditions or approvals. Cross-border transfers are permitted only where PDPL requirements are met, with stricter rules for certain data types and government data.

Organisations must identify a lawful basis for processing, provide clear privacy notices, manage vendors through contracts, conduct DPIAs for high-risk processing, implement security and breach-response measures aligned with applicable cybersecurity and sectoral requirements, and comply with any applicable data localisation obligations.

Data subjects have rights to be informed, to access and correct their data, and to request erasure where legally permitted, subject to statutory exceptions. The PDPL sets conditions, timelines and exemptions for these rights, requires documented handling of requests, and provides avenues for complaints to the competent authority, with sector regulators offering parallel remedies where applicable.

As a general checklist, organisations should operationalise the PDPL by inventorying and classifying data, documenting lawful bases (using compliant consent where required), publishing privacy notices and maintaining records of processing. They should establish governance (policies, roles, training), implement processor contracts and third-party controls, and align security and breach response with the NCA, SAMA and CST requirements, meeting the shortest applicable notification timeline.

1.3 Special Categories of Personal Data

Under the PDPL, "sensitive personal data" (including categories designated by law and regulation such as health, genetic and biometric data) may be processed only where a valid lawful basis exists and with heightened safeguards proportionate to risk, including stricter access controls, purpose limitation, minimisation, secure storage and transmission (eg, encryption), documented risk assessments for high-risk uses, tighter breach notification triggers, and additional conditions for disclosure and cross-border transfers. Certain unlawful disclosures of sensitive data can attract criminal liability.

For example, data about minors requires age-appropriate transparency and a lawful basis that typically includes verifiable consent of a parent or legal guardian, with special care to avoid unfair profiling or marketing and to implement enhanced protection by design and default. In addition, processing data relating to criminal accusations or convictions is generally limited to situations expressly authorised by law and typically carried out by or under the control of competent authorities, consistent with the Law of Criminal Procedure's constraints on the collection, access and disclosure of criminal case information and the Basic Law's privacy guarantees.

1.4 Processing of Personal Data for Research and Development Purposes

Companies providing products or services used by healthcare providers may only anonymise patient data when acting on the provider's documented instructions as the controller and on a valid lawful basis under the PDPL, with controller–processor roles, lawful bases and security/organisational measures set out in Article 1 (definitions), Articles 5–8 (lawful bases and consent) and Articles 10–12 (controller/processor obligations).

Once data is anonymised to a standard where an individual is not identifiable (and re-identification is not reasonably likely), they fall outside the PDPL's scope, but organisations must apply recognised de-identification methods and safeguards to prevent re-identification, as reflected in Article 1 of the PDPL (definition of personal data) read with its implementing regulations on anonymisation standards, and the NDMO Government Data Classification Policy and Anonymisation/De-identification guidance.

Secondary use for product development or scientific research must either be within the original purpose/notice and lawful basis or meet sectoral research/secondary-use conditions (including approvals under health research ethics rules), and processors may not repurpose data without explicit controller authorisation, consistent with Articles 5–8 (purpose/lawful basis/consent) and Articles 10–12 (processor limits) of the PDPL, and KSA health sector privacy and research governance instruments (eg, Saudi Health Council/National Health Information Center policies; Law of Ethics of Research on Living Creatures Articles 11–18 on IRB approval and consent/waivers). If data remains personal, full PDPL obligations continue to apply.

For EU-sourced datasets, KSA life sciences firms must comply with the European Health Data Space (EHDS) rules in addition to the European General Data Protection Regulation (GDPR), including data permits from Health Data Access Bodies, use of secure processing environments, purpose limitations and prohibited uses including re-identification bans, and output-only access, materially raising governance and security expectations for research and discovery pipelines that access EU electronic health data.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Although there is no horizontal AI statute, SDAIA published the AI Adoption Framework, which offers a guiding framework that provides a comprehensive roadmap for the adoption of AI in all sectors. Its goal is to provide necessary guidance and instructions, outline critical steps and procedures, and align with best practices to ensure optimal and responsible AI adoption, thus achieving successful milestones in the transformation towards AI within the ecosystem.

In September 2023, SDAIA published the first version of its AI Ethics Principles. These principles were issued and published with the aim of:

- supporting KSA's efforts towards achieving its vision and national strategies related to adopting AI technology, encouraging research and innovation, and driving economic growth for prosperity and development;
- developing and establishing AI ethics policies, guidelines, regulations and frameworks;
- governing data and AI models to limit the negative implications of AI systems and potential threats;
- helping entities adopt standards and ethics when building and developing AI-based solutions to ensure responsible use thereof; and
- protecting the privacy of data subjects and their rights with respect to the collection and processing of their data.

The AI Ethics Principles apply to all AI stakeholders designing, developing, deploying, implementing, using or being affected by AI systems within KSA, including, without limitation, public entities, private entities, non-profit entities, researchers, public services, institutions, civil society organisations, individuals, workers and consumers.

Seven principles are addressed in the framework:

- fairness;
- privacy and security;
- humanity;
- social and environment benefits;
- reliability and safety;
- transparency and explainability; and

- accountability and responsibility.

In addition, in November 2023, the government announced the establishment of the International Center for Artificial Intelligence Research and Ethics, which aims to advance competencies and legislative frameworks in the field of AI and other advanced technologies.

1.6 Data Breach Requirement

Under SDAIA's Personal Data Breach Incidents Procedural Guide, certain requirements must be adhered to in the event of a personal data breach, namely:

- *Stage one: Notify SDAIA within 72 hours.* Controllers must notify SDAIA via the Personal Data Breach Notification service on the National Data Governance Platform within no more than 72 hours of becoming aware of the breach, if the incident is expected to harm personal data or data subjects or conflict with their rights or interests, without prejudice to other NCA or sectoral reporting rules. The notification must include a description of the personal data breach (including timing, cause and discovery), the affected data subjects and data types, associated risks and mitigation measures taken and planned, whether data subjects have been or will be notified, and the relevant controller or data protection officer contact details.
- *Stage two: Breach incident containment.* Controllers must implement response and containment procedures for personal data breaches in line with international best practices and applicable regulations, including identifying the type and volume of affected data, determining and changing compromised data where possible, identifying affected individuals, and notifying data subjects without undue delay where their rights or interests may be harmed. Notifications must be made through appropriate communication channels, including direct and, where nationally widespread, public means, and must clearly explain the breach, associated risks, mitigation measures, controller and data protection officer contact details, and provide guidance to help affected data subjects mitigate potential harm such as fraud or identity theft.
- *Stage three: Documentation.* The controller must retain records of all personal data breach incidents,

including documents submitted to SDAIA, corrective actions taken and related records, and must implement necessary corrective measures to contain breaches based on lessons learned.

1.7 Regulators

KSA's data protection and cybersecurity oversight is shared across several authorities with distinct mandates. SDAIA is the primary regulator for the PDPL, while the NDMO sets national data governance policies. NCA issues cybersecurity baselines and controls, and sectoral regulators including SAMA, CST and the Capital Market Authority (CMA) impose parallel requirements within their domains. The framework relies on co-ordinated supervision, complaint-driven and risk-based enforcement, and the alignment of data, cybersecurity and sectoral standards.

Domestically, complaints are handled among the authorities in co-ordination with one another. Sector regulators impose domain-specific rules that intersect with data protection and cybersecurity. SAMA's core competence includes prudential and conduct supervision of financial institutions, with enforceable frameworks on cybersecurity, outsourcing and third-party risk that capture data handling and protection. CST supervises telecommunications, digital and cloud markets, including data localisation or transfer conditions embedded in licensing and cloud regulatory frameworks. CMA oversees capital markets participants, including data and cybersecurity requirements tailored to market integrity and investor protection.

SDAIA conducts and co-ordinates cross-border matters using a combination of PDPL powers over KSA-established controllers/processors, co-operation instruments with foreign authorities, and government-to-government channels where compulsion abroad is required. Typical triggers include referrals from foreign regulators, breaches involving offshore vendors or group entities, suspected unlawful international transfers, and data subjects' complaints with foreign elements.

In practice, significant privacy or security events often trigger multi-agency co-ordination. A personal data breach at a financial institution, for example, will require PDPL breach assessment and notifications

under SDAIA's remit, cyber-incident reporting and remediation under NCA controls, and sectoral reporting and corrective action under SAMA's frameworks.

1.8 Enforcement Proceedings and Fines

While the PDPL itself does not spell out detailed procedural steps for enforcement notices (such as how and when SDAIA must notify an organisation that it is under investigation), regulatory practice in KSA generally involves written notices or requests from the competent authority requiring production of documents or explanations.

How Cases Are Initiated

- Matters are commonly triggered by data subjects' complaints, breach/incident notifications and regulator-initiated supervision. SDAIA has been actively requiring prompt controller responses to complaints.

Notice and Response

- Authorities issue information requests and decisions, and may require corrective actions (eg, to cease or adjust processing, implement controls or register). Controllers must respond to requests from the competent authority and expect the authority's notice to set the deadline to respond. Failure to meet that deadline can trigger enforcement risk.
- Where a notification is required to SDAIA, the data controller must notify it within 72 hours of becoming aware of the breach. Where a notification is required to impacted data subjects, this must be made without undue delay.

Administrative Sanctions

- Warnings, corrective orders (including suspension/restriction of processing) and administrative fines up to SAR5 million, which may be doubled for repeat violations, may be issued. Decisions can include publication of a summary at the violator's expense.
- Administrative sanctions are appealable.

In addition, enforcement is administered through specialised committees established to review PDPL violations and impose the legally prescribed sanctions.

1.9 Enforcement Trends

The PDPL moved into active enforcement on 14 September 2024, under SDAIA, shifting the market from rulemaking to supervision and extending to non-KSA processors handling KSA residents' data. Recent trends under this Law highlight an increased focus on privacy protection in the digital space. This includes increased enforcement and regulatory scrutiny for privacy violations, and the law continues to evolve in line with technological advancements. In 2024, the government enhanced its monitoring of online platforms, and enforcement activity has increasingly intersected with cybersecurity incidents, such as hacking, illegal data interception and online harassment. Expect scrutiny of transfers, disciplined 72-hour breach reporting to SDAIA and timely data-subject notices, and supervisory use of the National Register and data privacy officer responsiveness as audit touchpoints.

Recent enforcement activity has also been reflected in committee decisions issued under the PDPL framework. During the past year, the committees issued 48 decisions confirming violations and imposing the legally prescribed penalties on regulated entities subject to the application of the PDPL. The violations reviewed by the committees included a number of practices related to the collection and processing of personal data, the disclosure of personal data without a legal basis, and failure by controllers to adopt appropriate organisational, administrative and technical measures to protect personal data, as well as violations relating to sending advertising and marketing messages to personal data subjects without obtaining their consent in accordance with the provisions of the Law.

2. Privacy Litigation

2.1 Privacy Litigation Overview

As of the time of writing, privacy-related litigation in KSA is still in its infancy. There have not been notable lawsuits related to the PDPL. However, complaints and regulatory actions relating to data breaches or violations of consent are starting to emerge, as highlighted in **1.9 Enforcement Trends**. Claimants are primarily individuals (data subjects/consumers, employees) alleging unlawful collection/use or disclosure.

Where disputes reach the courts, they typically arise in the context of unlawful access or disclosure of personal content, reputational harm, employment monitoring disputes, or broader civil liability claims relating to misuse of personal data, alongside criminal exposure under the Anti-Cyber Crime Law.

Currently, most actions relating to privacy protection are managed by SDAIA and the NDMO, which investigate complaints and enforce compliance with the PDPL. Instead of litigation, regulatory fines and investigations have been the primary mechanisms used to address violations.

As data protection awareness continues to rise and the enforcement of the PDPL strengthens, it is likely that litigation will increase. Businesses are expected to face greater scrutiny regarding data breaches and violations of data subjects' rights, which may lead to more litigation relating to compensation or damage claims in the future.

SDAIA is the primary authority for PDPL-related complaints, and its role will be critical in shaping the future of privacy-related litigation in KSA.

In addition, the Anti-Cyber Crime Law plays a significant role in privacy protection. Recent trends under this Law highlight an increased focus on privacy protection in the digital space. This includes heightened penalties for privacy violations, and the law continues to evolve in line with technological advancements. In 2024, the government enhanced its monitoring of online platforms, with an increasing number of cases involving cybercrime, such as hacking, illegal data interception and online harassment.

KSA courts may award compensation for material and non-material (moral) harm under general civil liability principles, assessed on a case-by-case basis. Relevant factors may include the nature and sensitivity of the data, the seriousness and duration of the violation, the extent of disclosure, the concrete impact on the individual (eg, distress or reputational injury), and the controller's fault and remediation.

In cross-border transfer arrangements, contractual safeguards (including standard contractual clauses

(SCCs)) may also allocate liability and compensation obligations between the contracting parties.

2.2 Recent Case Law

KSA courts publish selectively, and PDPL-specific private litigation is still nascent. As a result, the most influential privacy-related rules have emerged from: (i) criminal and quasi-criminal cases involving unauthorised access, disclosure or publication of personal content; (ii) defamation and reputational privacy decisions addressing online speech; (iii) labour and employment cases dealing with monitoring and employee data; and (iv) administrative/appeal rulings that review regulator measures on marketing, spam and data handling.

Given the limited publication of KSA judgments and the early stage of PDPL-specific private litigation, enforcement in practice has primarily been regulatory, through SDAIA and the committees reviewing violations under the PDPL framework.

Where claims are brought before courts, the PDPL recognises a right to seek proportionate compensation for material and moral damage before the competent court.

In addition, privacy-related disputes in the digital context may also involve criminal exposure under KSA's anti-cybercrime framework, particularly in incidents involving unauthorised access to, interception of or unlawful disclosure of private data.

2.3 Collective Redress Mechanisms

As of the time of writing, KSA does not have formal collective redress mechanisms for privacy-related violations, such as the class action system seen in some EU jurisdictions. The PDPL provides a robust framework for individual data protection, but it does not currently include provisions for collective actions or class actions for data privacy violations. Therefore, in privacy and data protection matters, collective redress is primarily sought through regulatory and administrative means rather than private, court-led class litigation.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Publicly available KSA case law specifically addressing “non-personal data” as a distinct category remains limited. Published jurisprudence generally addresses privacy or cybersecurity violations without parsing non-personal data as a separate doctrinal domain; disputes involving government open data, cloud data residency for non-personal content, or statistical disclosure control have not produced widely accessible precedent as of the time of writing. In practice, compliance assessments and dispute outcomes are guided by regulator-issued frameworks (SDAIA/NDMO, NCA, CST) and sectoral decisions rather than reported court opinions.

KSA does not maintain a single, comprehensive statute governing “non-personal data” as a distinct legal category. Instead, the treatment of non-personal data is shaped by a patchwork of sectoral and cross-cutting frameworks that regulate government and commercial data assets, cybersecurity and localisation, open data, data sharing and statistical data. While the PDPL governs personal data, non-personal data is principally governed through national data governance policies (issued by SDAIA/NDMO), open data and data sharing frameworks for public-sector information, cybersecurity baselines and cloud rules (NCA and CST), sector rules (notably statistics and some regulated industries), and general laws governing access to and protection of state or confidential information.

The PDPL seeks to regulate the collection, processing and storage of personal data in KSA, ensuring data privacy and security. This applies to all personal data, including data generated by Internet of Things (IoT) services, where the IoT is defined as sensors and devices (things) that are connected to the internet and/or other networks, which help to create value based on exchanged data such as easing jobs functions, as per the NCA’s Cybersecurity Guidelines for Internet of Things (“IoT Guidelines”). The IoT Guidelines aim to provide a comprehensive framework for organisations utilising IoT technologies to mitigate cybersecurity risks. The primary objective is to ensure that IoT

systems are secure, resilient, and compliant with the relevant laws and regulations.

The scope of the IoT Guidelines applies to all organisations in KSA that use IoT technologies, as well as IoT manufacturers developing products and services. The guidelines are non-mandatory but strongly recommended to minimise cybersecurity risks. They emphasise the importance of embedding cybersecurity into the governance, development, maintenance and management of IoT systems. The IoT Guidelines also encourage IoT manufacturers to adopt secure-by-design principles and provide consumers with transparent information about the cybersecurity features of their products. This dual focus on both users and manufacturers ensures a holistic approach to IoT cybersecurity.

From an international perspective, KSA has not enacted legislation comparable to the EU Data Act, nor has it announced plans to adopt a framework of similar scope.

3.2 Interaction of Data Regulation and Data Protection

Non-personal data is not subject to the PDPL’s lawful-basis regime. Its processing is governed by the NDMO’s National Data Governance Framework and standards, contractual obligations, sectoral rules and general KSA law. Entities must classify data, apply appropriate access controls and security measures, manage retention and disposal, and ensure data quality and integrity. To the extent that non-personal datasets derive from previously personal data, entities must document the anonymisation or aggregation process and maintain controls to prevent re-identification. Where non-personal data includes confidential business information or trade secrets, processing must comply with trade secret law and contractual confidentiality obligations. Cloud processing of non-personal data remains subject to the CST framework’s confidentiality, security and incident response requirements.

IoT service providers must ensure that users are informed and give explicit consent before their personal data is collected through IoT devices. The PDPL

requires that individuals have the right to access their data and request corrections.

Both IoT providers and data processors must implement robust security measures to protect data against breaches and unauthorised access, as stipulated in the NCA's guidelines. These obligations align with the PDPL's security provisions to prevent data breaches.

The PDPL mandates that personal data be destroyed when it is no longer necessary, which interacts with IoT providers' obligations to ensure that devices or systems do not retain unnecessary data. The interaction ensures that data protection is not overlooked as IoT technologies expand, balancing innovation with the protection of individuals' rights to privacy and security.

Under the PDPL, processing may rely on several bases, including consent, contractual or legal necessity, legitimate interests subject to a balancing test, vital and public interests, and research/statistics with appropriate safeguards. For each processing purpose, identify the primary legal basis, document the justification, apply purpose limitation and data minimisation, and maintain records of processing. Where relying on legitimate interests, complete and retain a written assessment demonstrating that the controller's interests are not overridden by the data subjects' rights and expectations and implement proportionate safeguards. For children's data and sensitive personal data, apply heightened controls, document the necessity and ensure enhanced security. Cross-border transfers require adequacy or appropriate safeguards and a transfer assessment on file, with derogations used only where strictly necessary.

3.3 Rights and Obligations Under Applicable Data Regulation

Non-Personal Data

With respect to non-personal data, organisations should align with the NDMO's data governance instruments (including the National Data Governance Interim Regulations, the Data Classification Policy, the Data Sharing Policy, the Open Data Policy and the KSA Open Data Licence), which require data to be classified and managed according to sensitivity and business/mission impact, and shared only on a pur-

pose-limited, proportionate and secure basis. Access and reuse are governed by the applicable data classification and any sharing agreement or open data licence, with "open" datasets generally made available under standardised terms that require attribution, prohibit misrepresentation and preserve data integrity. Fairness, transparency and non-discrimination principles apply to decisions on granting access, setting conditions or fees, and prioritising users, and charges (if permitted) should be objective and cost-reflective.

Requirements for the Collection, Processing and Use of Personal Data

Article 10 of the PDPL stipulates that the controller may collect personal data only from the personal data subject. Such personal data may only be processed for the purpose for which the personal data is collected. However, the controller, on an exceptional basis, may collect personal data from a person other than the personal data subject or process personal data for a purpose other than that for which the personal data is collected, namely when:

- the personal data subject consents in accordance with the provisions of the PDPL.
- the personal data is publicly available or collected from a publicly available source.
- the controller is a public entity, and the personal data was not collected, or processed, as required either for security purposes or in order to implement another law or fulfil judicial requirements in accordance with the provisions set out in the regulations;
- compliance with this restriction may cause harm to the personal data subject or affect the vital interests of the personal data subject (as set out in the regulations);
- collection or processing of personal data is necessary to protect public health or safety or to protect the life or health of a specific individual. The regulations shall set out the rules and procedures applicable in this respect;
- the personal data will not be recorded or stored in a form that makes it possible to identify the personal data subject directly or indirectly. The regulations set out the rules and procedures applicable in this respect; and

- collection of personal data is necessary to achieve the legitimate interests of the controller, provided that no sensitive personal data is processed and without prejudice to the rights and interests of the personal data subject.

Article 11 of the PDPL stipulates the following in relation to privacy, fairness and legitimate interest:

- The purpose for which personal data is collected must directly relate to the controller's purposes and must not contravene any applicable legal provisions.
- The methods and means of collecting personal data must:
 - (a) not conflict with any legal provisions;
 - (b) be suited to the circumstances of the personal data subject;
 - (c) be direct, clear and secure; and
 - (d) not involve any deception, misleading or extortion.
- The content of the personal data must be appropriate and limited to the minimum amount necessary to achieve the purpose of the collection. The regulations shall set out the rules applicable in this regard.
- If the personal data collected is no longer necessary for the purpose for which it has been collected, the controller must cease the collection and destroy the previously collected personal data.

Article 15 of the PDPL's implementing regulations also provides specifications relating to the collection of data from third parties, while Article 16 of the PDPL's implementing regulations addresses the processing of data, other than sensitive personal data, for legitimate interests by private entities. A legitimate interest is defined as any necessary interest of the controller that requires the processing of personal data for a specific purpose, provided that it does not adversely affect the rights and interests of the data subject.

Legitimate interests include, among others, the disclosure of fraud operations and the protection of network and information security. The controller may process personal data to achieve a legitimate interest provided that the processing purpose is legal, but in so far as the processing of data balances the rights and inter-

ests of the data subject with the legitimate interests of the controller, and, in doing so, the controller does not adversely affect the rights and interests of the data subject. Processing shall be within the reasonable expectations of the data subject.

Internal or External Privacy Policies

Article 12 of the PDPL stipulates that the controller shall adopt a personal data privacy policy and make it available to personal data subjects for review prior to collecting personal data. The policy shall specify the purpose of collection, the personal data to be collected, the method of collection, the means of storage and processing, the manner in which the personal data shall be destroyed, and the rights of the personal data subject in relation to the personal data and how such rights shall be exercised.

Data Subjects' Access Rights

Article 5 of the PDPL states that a data subject has the right to access their personal data available with the controller provided that such access does not negatively impact the rights of others, such as intellectual property rights or trade secrets. Article 6 also makes it clear that, subject to certain parameters, data subjects have the right to request a copy of their personal data in a readable and clear format from the controller.

Article 13 of the PDPL stipulates that when collecting personal data directly from the personal data subject, the controller shall take appropriate measures to inform the personal data subject of the following prior to collection:

- the legal basis and valid practical reasons for collecting their personal data;
- the purpose of the collection, whether collecting some or all of the personal data is mandatory or optional, and that the personal data collected will not be subsequently processed in a manner inconsistent with the collection purpose or in circumstances other than those stated in Article 10 of the PDPL;
- the identity of the person collecting the personal data and the address of such person's representative, if necessary (unless the collection is for security purposes);

- the entities to which the personal data will be disclosed, the capacity of such entities, and whether the personal data will be transferred, disclosed or processed outside KSA;
- the potential consequences and risks that may result from not collecting the personal data;
- the rights of the personal data subject pursuant to Article 4 of the PDPL; and
- such other elements as set out in the regulations based on the nature of the activity performed by the controller.

3.4 Regulators and Enforcement

For non-personal data, the NDMO leads data governance and classification (particularly for government datasets), alongside the Digital Government Authority (DGA) on public-sector data and open data. The CSA's cloud and data localisation frameworks and the NCA's baseline controls shape non-personal data handling across sectors, with sector regulators (SAMA, CMA, health regulators) embedding these standards in outsourcing, resilience and information-management rulebooks. Co-ordination relies on inter-agency standards alignment and cross-referrals where cloud, telecom and sector supervision overlap, and the General Authority for Competition (GAC) may engage where control of large non-personal datasets or infrastructure access raises competition concerns. Recent trends include heightened scrutiny of cloud and data localisation, deeper embedding of NCA controls in sectoral rulebooks, and continued standardisation of government data governance and open data practices through SDAIA/NDMO and DGA.

For personal data, SDAIA and its Personal Data Protection Authority (PDPA) are the primary regulators of the PDPL, with the CSA supervising telecom, digital and cloud frameworks (including data residency and anti-spam) and NCA overseeing cross-sector cybersecurity controls. Sector regulators – most notably SAMA and CMA – set complementary requirements on data security, outsourcing/cloud, operational resilience and third-party risk. In health, the Ministry of Health and national health information bodies govern health data handling and exchange. Public prosecution addresses criminal aspects of data offences. Co-ordination occurs via referrals, co-operation agreements, concurrent investigations and aligned

guidance – for example, SDAIA/PDPA handling privacy compliance, NCA overseeing security baselines, CST supervising cloud/telecom obligations and sector regulators applying domain-specific controls – with GAC interfacing on digital-market issues and co-ordinating to ensure remedies respect privacy and sectoral rules. Recent trends include maturation of PDPL guidance and stepped-up supervisory engagement by SDAIA/PDPA, convergence of incident reporting expectations, and a growing GAC focus on data-driven theories of harm in digital and fintech markets.

Sector authorities (CST, SAMA, health regulators, others) typically cross-reference NDMO data governance standards for classification, sharing and life-cycle management and align security expectations with NCA controls. This creates a layered regime where sectoral enforcement incorporates national data governance baselines.

DGA government/open-data mandates align with NDMO standards for classification, metadata and sharing; where publication risks re-identification, DGA processes incorporate de-identification and licensing controls consistent with national guidance.

NCA co-ordinates cybersecurity oversight with sector regulators (harmonised audits and incident reporting) and aligns protection levels with national classification schemes.

CST co-ordinates with SDAIA on data residency, access by public authorities, and security obligations that apply across data types. CST also interfaces with GAC when telecom/information/communications/technology and cloud matters raise data-related competition issues.

GAC consults SDAIA and sector regulators on technical feasibility of data access, segregation, interoperability or de-identification in conduct cases and merger remedies involving datasets.

4. Sectoral Topics

4.1 Use of Cookies

As of the time of writing, there are no specific requirements imposed in KSA for the use of cookies. For the general rules in relation to gaining consent in relation to cookies and SDKs, please see **3.3 Rights and Obligations Under Applicable Data Regulation** under ‘Requirements for the Collection, Processing and Use of Personal Data’.

4.2 Personalised Advertising and Other Online Marketing Practices

In KSA, personalised/targeted advertising is principally governed by the PDPL, together with CST rules on electronic marketing and anti-spam, and the E-Commerce Law and its Implementing Regulations. The PDPL generally requires explicit consent before personal data may be used for direct or targeted marketing, particularly where there is no prior interaction with the individual, and individuals must be given a clear and easy way to withdraw consent at any time, particularly when advertising is delivered through personal communication channels such as email or SMS, and individuals must be given a clear and easy way to withdraw consent at any time.

CST’s commercial communications and anti-spam framework requires prior opt-in for promotional SMS, calls and electronic messages, sender identification, and a free, effective opt-out that is promptly honoured, alongside suppression-list management. For online tracking, consent is expected for advertising cookies/SDKs and cross-site identifiers, delivered through a compliant consent interface that is granular, informed and reversible. Cross-border transfers must meet PDPL transfer conditions and be governed by appropriate contractual safeguards.

While the law does not expressly regulate “profiling” in the same way as the EU GDPR, any profiling or targeting that involves personal data must comply with the PDPL’s general principles of lawful processing, transparency and consent. The use of sensitive personal data (such as health, biometric, genetic or religious data) for marketing purposes is prohibited. Children’s personal data is protected under the general PDPL

regime, and marketing involving minors requires valid consent, typically from a parent or legal guardian.

4.3 Employment Privacy Law

Under the PDPL, employers are considered controllers, and therefore employee and applicant data must be processed lawfully, fairly and transparently, and only for specific and legitimate purposes in accordance with the PDPL. Monitoring time or productivity tracking must be necessary and proportionate, explained in clear notices and grounded on a suitable lawful basis. High-risk monitoring should be supported by documented risk assessments, and biometric time clocks involving sensitive data require enhanced safeguards.

Remote work should implement technical and organisational measures, respect localisation/transfer limits, and avoid excessive location/activity tracking beyond stated purposes. In remote-work settings, employers commonly apply technical and organisational safeguards, including access controls, encryption, secure connectivity and logging-in in line with NCA expectations, while taking care to limit location or activity tracking to what is reasonably required for defined purposes. Organisations should also ensure that any processing or storage outside KSA complies with PDPL cross-border transfer conditions (including where employee data is accessed remotely from abroad, which may constitute a cross-border transfer), and associated regulatory safeguards.

Bring Your Own Device (BYOD) programs warrant particular care: mobile device management or secure containers should segregate corporate from personal data; access to personal content should be tightly limited; and any device-level monitoring or telemetry must be clearly disclosed and confined to security-necessary data, reflecting the PDPL’s data-minimisation and purpose-limitation principles.

In addition to PDPL compliance, many KSA organisations are already aligning BYOD security controls with NCA standards, because insecure personal devices can expose personal data to breaches and lead to PDPL compliance violations. The use of corporate IT systems is best governed through cogent, well-publicised acceptable-use and monitoring policies that

set expectations for permissible activities, monitoring scope and retention.

Regarding applications, employers may verify candidates' education, employment history or other relevant records, but such processing must be lawful, transparent and limited to legitimate purposes. Sensitive data, such as criminal records or health information, generally requires explicit consent, and any third-party verification providers or processors must comply with PDPL standards.

4.4 Data Protection in M&A

SDAIA, the PDPL and the national cybersecurity base-lines govern personal data handling across M&A from diligence through integration. Controllers must rely on a valid lawful basis, respect purpose limitation and minimisation, and implement safeguards (access controls, encryption, logging in).

During diligence, entities should limit and structure disclosures and use redaction, aggregation or anonymisation, apply heightened controls for sensitive data, and consider a DPIA where risks are high. Cross-border disclosures must satisfy PDPL transfer conditions with contractual safeguards, and parties should clearly allocate roles including processors of such data.

At change of control, the buyer should confirm that personal data will continue to be processed for compatible purposes on a valid legal basis (eg, legitimate interests where applicable) and assess whether refreshed consents are needed if purposes or disclosures materially change. Controllers must ensure transparency by updating privacy notices and, where required, informing data subjects of any change to the data controller, processing purposes or material recipients.

Post-closing integration should be preceded by a DPIA for new or high-risk uses, alignment of retention schedules, migration and segregation controls, and the execution or novation of compliant data processing agreements with vendors. Buyers should also update records of processing activities, appoint or confirm a data officer if required, implement mechanisms to honour data subjects' rights, and ensure that

any ongoing cross-border transfers after integration meet PDPL transfer conditions.

5. International Considerations

5.1 Restrictions on International Data Transfers

KSA regulates cross-border transfers through the PDPL for personal data, complemented by sectoral and horizontal frameworks that affect non-personal data, including rules issued by SAMA for financial services, CST regulations regarding cloud computing services for telecom and cloud, health sector regulations, NDMO frameworks for government and "official" data, and NCA controls. Together, these instruments function as approval, assurance or localisation frameworks depending on the data and the regulated entity.

For both personal and non-personal data, a "transfer" is understood broadly. It generally includes hosting or storing data outside KSA, enabling remote access to KSA-hosted data by personnel located abroad (for example, for support or shared services), making data available to or sharing it with foreign controllers, processors or sub-processors (including group affiliates), and any onward disclosure by a foreign recipient to another foreign party. Sectoral guidance, particularly for cloud and outsourcing, treats remote administration and sub-processing outside KSA as cross-border activity and therefore subject to transfer controls.

Transferring personal data outside KSA involves moving individuals' personal data from KSA to another country or jurisdiction. This process is often necessary for global business operations, partnerships or service delivery (eg, while using cloud storage solutions). Such arrangements are subject to specified requirements of the PDPL.

The NDMO sets out general standards for personal data transfer beyond the geographical limits of KSA in order to specify the terms and conditions for cross-border transfer and storage of personal data for both public and private entities while pointing out the sovereignty of personal data. The standards also stipulate the rights of personal data owners, along with general

guidelines and exceptions for personal data transfer beyond KSA's borders – thereby creating secure processing for personal data.

The Regulation on Personal Data Transfer Outside the Kingdom (“Transfers Regulation”) imposes several restrictions on the international transfer of personal information to ensure that such transfers comply with KSA's data protection standards. According to Article 29 of the PDPL, personal data may only be transferred outside KSA if the receiving country or entity provides an appropriate level of protection that meets or exceeds the standards set by KSA law. This requirement is further detailed in Article 3 of the Transfers Regulation, which mandates that the competent authority publish and maintain a list of countries or international organisations that meet these protection standards. If the receiving country is not on this list, the transfer is generally prohibited unless specific appropriate safeguards are implemented, such as SCCs, BCR, or approval certificates from a licensed body as outlined in Article 4. These safeguards ensure that the data is protected to a level consistent with KSA regulations, even when transferred internationally.

Before transferring personal data outside KSA, controllers are required to conduct a risk assessment under Article 7 of the Transfers Regulation. This assessment is mandatory for transfers involving sensitive data or when the transfer is made under the exemptions specified in Article 4 of the Transfers Regulation. The risk assessment must evaluate several factors, including the purpose and legal basis for the transfer, the nature of the data, and the appropriate safeguards in place to protect the data. Additionally, the assessment must consider the potential material or moral effects of the transfer and the likelihood of risks to data subjects. This ensures that controllers carefully weigh the necessity of the transfer against the potential risks to individuals' privacy and data security. The risk assessment requirement underscores the importance of ensuring that international transfers are conducted responsibly and in compliance with the Transfers Regulation.

Furthermore, the Transfers Regulation allows for exemptions from the general restrictions on inter-

national data transfers in specific cases, as outlined in Article 4 (2). For example, transfers are permitted for central operations within multinational entities, for scientific research, or to provide services to data subjects, provided that the appropriate safeguards are in place. However, even in these cases, the data must be limited to the minimum amount necessary to achieve the intended purpose, and the receiving entity must ensure compliance with KSA data protection standards. If the competent authority determines that the safeguards are inadequate, the transfer may be halted, and the controller must notify the relevant entities under Article 6 of the Transfers Regulation. These restrictions and requirements ensure that international data transfers are conducted in a manner that prioritises the protection of personal data and aligns with KSA's legal and regulatory framework.

5.2 Government Notifications and Approvals

Government approval for certain international data transfers is required under the Transfers Regulation. Transfers to countries or organisations on the competent authority's approved list under Article 3 (1) do not need additional approval, but transfers to non-listed countries require appropriate safeguards, such as SCCs or BCR, which may need to be reviewed or approved. As of the time of writing, such a list of countries is yet to be published.

For specific cases such as scientific research or providing services to data subjects, the receiving entity must hold an approval certificate from a licensed body under Article 4 (2)(E), provided that the transferred data is not sensitive data. Additionally, controllers must conduct a risk assessment for sensitive data transfers per Article 7.

While not all transfers require explicit approval, the Transfers Regulation ensures oversight through conditions such as exemptions from such approvals and the potential revocation of such exemptions if the instated safeguards are inadequate. Controllers must ensure compliance with the Transfers Regulation, which may involve notifying or seeking approval from the competent authority, particularly for sensitive data or transfers to non-approved jurisdictions. This framework prioritises data protection while allowing international transfers under strict safeguards.

5.3 Data Localisation Requirements

The PDPL does not stipulate that data must be localised provided that the transfer and processing of personal data outside KSA is performed in accordance with the PDPL and any other applicable law or regulation applicable to such personal data in KSA. In addition, accessing data remotely would still constitute a transfer under the Standard Contractual Clauses For Personal Data Transfer.

When transferring personal data outside KSA, there are special rules and regulations, however, that may apply in addition to, and exclusive of, the PDPL depending on the type of data (eg, health data) or sector (eg, financial), or if the localisation of data is in the national security, or public, interest of KSA. Under such circumstances, the transfer and/or processing of personal data may be restricted or prohibited altogether.

From a PDPL perspective, per the Transfers Regulation, there are no distinct rules for transferring data relating to particular sectors; instead, the Transfers Regulation categorises certain types of data as sensitive, which are subject to stricter transfer requirements. Otherwise, data transfers outside KSA may be permitted subject to certain circumstances. For example, Article 4 (2)(C) allows the transfer of sensitive data for central operations within multinational entities, provided that the controller adheres to BCR or SCCs to ensure data protection. Similarly, Article 4 (2) (E) permits the transfer of sensitive data for scientific research and studies, but only if the data is limited to the minimum amount required and the receiving entity has an approval certificate from a body licensed by the competent authority.

Additionally, Article 7 addresses the transfer of sensitive data on a continuous or widespread basis, requiring controllers to conduct a risk assessment before such transfers. This risk assessment must evaluate the purpose and legal basis of the transfer, the nature of the data, and the appropriate safeguards in place to ensure compliance with the Transfers Regulation. While the Transfers Regulation does not explicitly differentiate between sectors, it imposes stricter requirements for sensitive data, which often includes sector-specific information such as health records or

financial data. By requiring SCCs, BCR or approval certificates, the Transfers Regulation ensures that all sensitive data, regardless of its sector, is transferred outside KSA only under conditions that guarantee an appropriate level of protection.

The Transfers Regulation sets out the provisions in cases where controllers are exempted from the requirements to comply with the level of protection and the minimum level of transfer of personal data stipulated in subparagraphs (b) and (c) of paragraph (2) of Article (29) of the PDPL and provisions of the Transfers Regulation, namely that there is an adequate level of protection for personal data outside KSA and the transfer is limited to the minimum amount of personal data needed.

5.4 Blocking Statutes

KSA has no single “blocking statute”, but it has various relevant legal authorities on internet censorship which are primarily aimed at controlling online content to align with the country’s cultural, religious and legal norms. Key legislation on web censorship includes:

- **ACC Law:** Article 6 of the ACC Law prohibits, and prescribes imprisonment and fines as penalties for, the publication, dissemination or promotion of content deemed offensive to public order, religious values or national security. This includes content relating to pornography, gambling, blasphemy, defamation and political dissent.
- **TCIT Law:** Article 24 of the TCIT Law stipulates that, after co-ordination with the competent authorities, the CST must:
 - (a) introduce internet filtering and limit access to specific content on the internet; and
 - (b) prevent or restrict access to internet services by using internet gateways.

It is prohibited to by-pass or swindle internet filtering or to provide the means to do so. In addition, the CST shall set the regulating controls and requirements.

Foreign subpoenas and discovery orders are not self-executing in KSA and ordinarily must proceed through letters rogatory or treaty channels. Applications for the enforcement of foreign judgments and arbitration awards under the Execution Law must be

submitted to the judge of the Execution Court with jurisdiction over such matters, to ensure their enforceability.

For sanctions compliance, internal screening is generally feasible, but outward disclosures – especially to foreign public authorities – must rely on a PDPL legal basis and a permitted transfer mechanism and, in regulated sectors (notably financial services), must use KSA-mandated domestic reporting gateways rather.

KSA has shifted to a modern, safeguards-based cross-border regime under the PDPL, with transfers permitted via adequacy, appropriate safeguards or narrow derogations, subject to risk assessment and accountability. The most impactful next step will be publication of an adequacy list further defining the role of a data protection officer.

5.5 Recent Developments

Since 2023, there have been no significant changes to KSA's data protection laws and regulations, with the primary framework still largely governed by the PDPL, which was designed to align with international data protection standards. Nevertheless, the most notable development in KSA's data protection regime occurred on 14 September 2024, when the PDPL finally became fully enforceable, marking a significant milestone for businesses operating in KSA. This full enforcement deadline required organisations to ensure compliance with the Law's provisions, including implementing robust data protection measures, appointing data protection officers and adhering to strict data transfer requirements. On 27 April 2025, SDAIA launched its third public consultation on the PDPL and its regulations proposing some amendments, but as of the time of writing nothing has been finalised.

Law and Practice

Contributed by:

Vladimir Djerić, Lena Petrović and Katarina Radović
Mikijelj, Janković & Bogdanović

Contents

- 1. Legal and Regulatory Framework p.396**
 - 1.1 Overview of Data and Privacy-Related Laws p.396
 - 1.2 Rights and Obligations p.397
 - 1.3 Special Categories of Personal Data p.397
 - 1.4 Processing of Personal Data for Research and Development Purposes p.398
 - 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.398
 - 1.6 Data Breach Requirement p.398
 - 1.7 Regulators p.398
 - 1.8 Enforcement Proceedings and Fines p.399
 - 1.9 Enforcement Trends p.399
- 2. Privacy Litigation p.400**
 - 2.1 Privacy Litigation Overview p.400
 - 2.2 Recent Case Law p.400
 - 2.3 Collective Redress Mechanisms p.400
- 3. Requirements for the Protection and Processing of Non-Personal Data p.400**
 - 3.1 Objectives and Scope of Data Regulation p.400
 - 3.2 Interaction of Data Regulation and Data Protection p.400
 - 3.3 Rights and Obligations Under Applicable Data Regulation p.400
 - 3.4 Regulators and Enforcement p.401
- 4. Sectoral Topics p.401**
 - 4.1 Use of Cookies p.401
 - 4.2 Personalised Advertising and Other Online Marketing Practices p.401
 - 4.3 Employment Privacy Law p.401
 - 4.4 Data Protection in M&A p.401
- 5. International Considerations p.402**
 - 5.1 Restrictions on International Data Transfers p.402
 - 5.2 Government Notifications and Approvals p.403
 - 5.3 Data Localisation Requirements p.403
 - 5.4 Blocking Statutes p.403
 - 5.5 Recent Developments p.403

Mikijelj, Janković & Bogdanović is a Belgrade-based law firm established in 1985, with a long-standing practice in dispute resolution, intellectual property, and regulatory matters. The firm's data protection and privacy work is handled by a dedicated team of three lawyers, including two partners and a senior associate. The team advises domestic and international clients on compliance with the Serbian Personal Data Protection Act, cross-border data transfers, data breach response, employment-related data process-

ing, and privacy issues arising in media, advertising, and digital services. The firm has experience advising clients operating in the telecommunications, pharmaceuticals, online commerce, gambling, and media sectors. The data protection practice works closely with the firm's dispute resolution, employment, IP, and corporate teams, allowing it to address data protection issues arising in regulatory proceedings, commercial transactions, and litigation.

Authors



Vladimir Djerić is a partner at Mikijelj, Janković & Bogdanović. He advises clients on dispute resolution, media law, data protection and privacy. Vladimir represents clients in court disputes involving privacy,

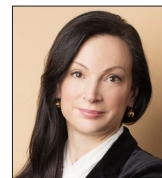
defamation, and freedom of expression. His practice includes advising media organisations, technology companies, and regulated businesses on compliance and litigation risk related to personal data processing. He is a member of the Belgrade Bar Association.



Lena Petrovic is a senior associate at Mikijelj, Janković & Bogdanović. She advises clients on data protection and privacy, advertising law, dispute resolution, media law and intellectual property. Lena works on GDPR-

aligned compliance under Serbian law, international data transfers, direct marketing practices, and

privacy issues arising in digital and media projects. She assists clients in regulatory proceedings and litigation involving personal data protection. She also represents clients in proceedings before the Commissioner for Information of Public Importance and Protection of Personal Data. Lena is a member of the Belgrade Bar Association.



Katarina Radovic is a partner at Mikijelj, Janković & Bogdanović. Her practice focuses on employment law, data protection, dispute resolution, and intellectual property. Katarina advises employers on the lawful

processing of employee data, workplace monitoring, internal investigations, and data protection compliance in HR-related processes. She has experience representing clients in administrative and court proceedings concerning personal data protection and employment disputes. Katarina is a member of the Belgrade Bar Association.

Mikijelj, Janković & Bogdanović

Vlajkovicева 28
11000 Belgrade
Serbia

Tel: +381 11 3231 970
Fax: +381 11 3245 065
Email: office@mjb.rs
Web: www.mjb.rs



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The protection of personal data in Serbia is grounded in constitutional, statutory, and sector-specific sources. The Constitution of the Republic of Serbia guarantees the protection of personal data and the confidentiality of communications, allowing limitations only under strict legal and judicial conditions. The Constitution of the Republic of Serbia contains several provisions relating to the protection of privacy, including the confidentiality of letters and other means of communication (Article 41 of the Constitution) and the protection of personal data (Article 42 of the Constitution).

Under the Constitution, the confidentiality of letters and other means of communication may only be derogated from for a specified period of time and based on a court decision for the purpose of conducting criminal proceedings or protecting the safety of Serbia, in a manner stipulated by the law (Article 41 of the Constitution).

The Constitutional guarantee of protection of personal data (Article 42 of the Constitution) provides that use of personal data for any purpose other than that for which it was collected is prohibited and punishable in accordance with the law, unless it is necessary to conduct criminal proceedings or protect the safety of Serbia, in a manner stipulated by the law.

The Constitution also guarantees that everyone has the right to be informed of the collection of personal data relating to them, in accordance with the law, as well as the right to court protection in the event of abuse of their personal data. The primary statute is the Personal Data Protection Act (PDPA), applicable since 2019, which is largely aligned with the GDPR and the EU Law Enforcement Directive.

The PDPA applies across sectors and governs the processing, storage, and international transfer of personal data. The solutions provided by the PDPA are in line with the GDPR. The PDPA defines personal data, the different types of personal data and the manner of their collection, processing and transfer outside of

the territory of Serbia. The PDPA has limited extraterritorial reach and applies to foreign controllers offering goods or services to individuals in Serbia or monitoring their behaviour. While Serbia does not regulate non-personal data or AI through binding legislation, data protection rules apply where AI systems rely on personal data, and policy alignment with EU developments is ongoing. In August 2023, Serbia adopted the Personal Data Protection Strategy for the period from 2023 to 2030. The main goal of this Strategy is “[r]especting the right to protection of personal data in all areas of life”.

Provisions that are of relevance to the protection of personal data may also be found in the Electronic Communications Act (ECA), as well as in sector-specific legislation, such as the Act on Health Documents and Records, the Act on Records and Data Processing in Interior Affairs, the National DNA Registry Act and the Law on Social Cards.

Also, the provisions of the Information Security Act (ISA) regarding data breach reporting and notification are relevant for protection of personal data and privacy. The ISA regulates (i) measures for protection against the security risks in ICT systems, (ii) the liability of legal entities in relation to the management of ICT systems, and (iii) the use of ICT systems and the competent authorities in charge of implementation of protective measures (Article 1 of the ISA).

The operators of the ICT systems of essential services are obliged to notify RATEL, as the national CERT, of incidents and attacks related to the ICT system that may have a significant impact on informational security. An incident must be reported in writing to the national CERT within one day of its occurrence. If it relates to the secret data, the operator of the ICT system of special importance is also obliged to follow the rules on data secrecy (Article 11 of the ISA).

If the reported incident is of a public interest, RATEL may order its public disclosure. If the incident is related to crimes prosecuted ex officio, RATEL shall inform the competent Public Prosecutor’s Office and/or the Ministry of the Interior. If the incident involves a violation of personal data, RATEL will report the incident

to the Commissioner for Protection of Personal Data (Article 11 of the ISA).

According to the Constitution of Serbia, ratified international treaties and generally accepted rules of international law are part of the legal system of Serbia, and laws and other general acts enacted in Serbia have to comply with ratified international treaties and generally accepted rules of international law (Article 194 of the Constitution).

In the context of personal data protection, Serbia has ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows (ETS No 108, Strasbourg, 28 January 1981) (the "Convention"). The Convention serves as a legal ground for transfer of data from Serbia to the UK after Brexit, since the UK is party to it and signatories of the Convention are considered to be countries that ensure an adequate level of data protection.

Serbia is also a signatory to various international agreements that contain provisions that could be relevant for accessing or obtaining data processed in the territory of Serbia, mostly in the context of international co-operation in civil and criminal matters.

Because Serbia is in the process of accession to the EU, much Serbian legislation focuses on the implementation of the standards and provisions provided by EU legislation.

Moreover, the PDPA contains solutions provided by the GDPR and the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (the Police Directive).

1.2 Rights and Obligations

Personal data processing in Serbia is governed by the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

Processing must rely on a valid legal basis, such as consent, contractual necessity, legal obligation, legitimate interest, or public interest.

Data subjects have rights to access, rectification, erasure, restriction, portability, objection, and protection against automated decision-making. Organisations must implement appropriate technical and organisational measures and maintain internal accountability.

Key compliance obligations include:

- maintaining records of processing activities;
- implementing data protection by design and by default;
- appointing a data protection officer (DPO) where required;
- concluding data processing agreements;
- adopting breach response procedures; and
- conducting data protection impact assessments where high-risk processing is involved.

1.3 Special Categories of Personal Data

Special categories of personal data include personal data on racial or ethnic origin, political opinion, religious or philosophical belief, or trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health; or data concerning a natural person's sex life or sexual orientation. Their processing is generally prohibited unless a specific statutory exemption applies, such as explicit consent, employment law obligations, public health interests, or legal claims.

Processing of data relating to criminal convictions and offences is permitted only under the control of competent authorities or where expressly authorised by law.

Consent for data processing is valid if it is given by a person of 18 years of age or older. Data concerning minors requires heightened protection, and consent must be obtained from a parent or legal guardian when information society services are offered directly to children. Exceptionally, persons aged 15 years or older are able to give consent in relation to online services.

1.4 Processing of Personal Data for Research and Development Purposes

Companies providing digital tools or technologies used in healthcare may process patient data for research and development purposes if a valid legal basis exists and appropriate safeguards are applied, in accordance with the PDPA.

Scientific and statistical research may rely on legal obligations, public interest, or consent, provided data minimisation and confidentiality are ensured. Serbia does not yet have legislation comparable to the European Health Data Space Regulation, but alignment is expected as part of EU accession.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Serbia does not currently have binding AI legislation. However, the use of AI systems involving personal data remains subject to the PDPA. Controllers must ensure transparency, purpose limitation, data accuracy, and proportionality when training or deploying AI models.

Automated decision-making that produces legal or similarly significant effects is restricted unless based on explicit consent, contractual necessity, or legal authorisation, with safeguards including human intervention. Serbia's 2025–2030 AI Strategy envisages the adoption of comprehensive AI legislation by 2027, likely reflecting a risk-based approach similar to the EU AI Act.

In practice, organisations are expected to implement internal governance, bias mitigation, explainability measures, and human oversight when AI systems process personal data.

1.6 Data Breach Requirement

In the event of a personal data breach, controllers must notify the Commissioner without undue delay and, where feasible, within 72 hours after becoming aware of the breach. Notification to affected data subjects is required if the breach is likely to result in a high risk to their rights and freedoms.

The notification must describe the nature of the breach, likely consequences, and measures taken or

proposed to mitigate harm. Controllers must document all breaches internally, regardless of notification obligations.

Data breaches may trigger inspections by the Commissioner, co-ordination with the national CERT under the Information Security Act, and potential misdemeanour proceedings.

1.7 Regulators

The primary supervisory authority is the Commissioner for Information of Public Importance and Protection of Personal Data. Under the PDPA, the Commissioner is a supervisory body that:

- monitors and enforces the application of the PDPA;
- advises the national parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
- provides information to any data subject concerning the exercise of their rights under the PDPA; and
- co-operates with the supervisory authorities of other states.

The Commissioner also:

- handles complaints lodged by a data subject;
- prepares standard contractual clauses and authorises contractual clauses that would serve as an adequate safeguard for the transfer of data to a country or international organisation that does not ensure adequate levels of protection of personal data;
- establishes and maintains a list in relation to the requirements for a data protection impact assessment when required by law; and
- accredits certification bodies, issues certifications and approves criteria of certification (Article 78 of the PDPA).

Data Protection Commissioner Powers

The Commissioner is vested with a set of investigative powers, corrective powers and advisory powers that are identical to the powers of the supervisory body prescribed by the GDPR. The Commissioner is authorised, inter alia, to:

- order the data controller or data processor to provide information it requires for the performance of its tasks;
- monitor the application of the provisions of the PDPA by exercising its inspection powers;
- carry out a review on certifications issued in accordance with the PDPA;
- obtain access to any premises of a controller or processor, including to any data-processing equipment and means;
- issue reprimands to a controller or processor where processing operations have infringed provisions of the PDPA;
- order the controller or the processor to comply with the data subject's requests to exercise their rights pursuant to the PDPA;
- order the controller or processor to bring processing operations into compliance with the provisions of the PDPA, where appropriate, in a specified manner and within a specified period;
- order the controller to communicate a personal data breach to the data subject;
- impose a temporary or definitive limitation, including a ban on processing;
- order the rectification or erasure of personal data or restriction of processing;
- withdraw a certification or order the certification body to withdraw an already-issued certification;
- impose an administrative fine – in addition to, or instead of, other corrective measures – depending on the circumstances of each individual case; and
- order the suspension of data flows to a recipient in a third country or to an international organisation (Article 79 of the PDPA).

Other authorities with overlapping competences include RATEL (telecommunications and cybersecurity incidents), sectoral regulators, and courts. Proceedings are typically triggered by data subject complaints, breach notifications, or ex officio inspections. Guidance issued by the Commissioner is formally non-binding but is treated as authoritative in practice and frequently relied upon by courts and public bodies.

1.8 Enforcement Proceedings and Fines

Under the PDPA, the Commissioner is authorised to exercise its powers in accordance with the Adminis-

trative Procedure Act and Inspection Act (Article 77 of the PDPA) as well as to initiate proceedings before the courts and other competent bodies in accordance with the law (Article 79 of the PDPA).

The Commissioner is obliged to act upon the complaints of a data subject and initiate the inspection procedure, as well as to inform the data subject about the outcome of the inspection and their right to initiate administrative court proceedings against the decision of the Commissioner. If the data subject is not satisfied with the decision of the Commissioner, or if the Commissioner fails to act upon the complaint within 60 days from its receipt, the data subject is authorised to initiate court proceedings against the Commissioner in accordance with the Administrative Court Proceedings Act (Articles 82 and 83 of the PDPA).

The enforcement of personal data protection is the remit of the Commissioner, who is authorised to investigate whether data processing is lawful, including the right to request access to the premises of the data controller and means of data processing, as well as to order rectification of identified irregularities in data processing within a specified period of time, or to render a temporary ban on any processing carried out contrary to the provisions of the PDPA (Article 79 of the PDPA).

Data processing contrary to the provisions of the PDPA represents a misdemeanour punishable with a fine between RSD50,000 and RSD2 million for a legal entity, RSD20,000 and RSD500,000 for an entrepreneur, and RSD5,000 and RSD150,000 for both a natural person and the responsible person in a legal entity (Article 95 of the PDPA).

1.9 Enforcement Trends

Enforcement activity in Serbia remains moderate and largely corrective rather than punitive. Recent trends show a focus on failure to maintain records, lack of DPO appointments, insufficient transparency, and inadequate security measures. Large-scale fines remain uncommon, and enforcement is often complaint-driven.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Two main pieces of legislation relevant for privacy litigation in Serbia are the PDPA and the Law on Public Information and Media. The PDPA defines data subjects' rights and mechanisms for their protection, with the Commissioner as the main authority for the protection of personal data. Serbia has a modest number of cases related to the protection of personal data. However, there are numerous defamation cases governed primarily by the provisions of the Law on Public Information and Media.

Privacy litigation in Serbia remains limited compared with that in EU member states. Most disputes arise in the context of media reporting, defamation, and alleged violations of privacy under the Law on Public Information and Media.

Non-material damage is compensable under general tort law, and courts may award damages for emotional distress or reputational harm. Strategic lawsuits against public participation (SLAPPs) targeting journalists and media outlets have increased in recent years.

Since Serbia is not a member of the EU, EU case law does not directly affect Serbian courts. However, decisions of the ECHR are relevant in domestic court cases and are taken into account, particularly in the interpretation and application of the provisions of the European Convention on Human Rights.

2.2 Recent Case Law

There is limited case law directly interpreting the PDPA. However, court decisions and regulatory practice increasingly reference ECHR jurisprudence on privacy and freedom of expression.

Cases involving investigative journalism platforms have shaped the balance between public interest reporting and privacy rights, confirming that public figures enjoy a lower expectation of privacy when reporting serves democratic oversight.

2.3 Collective Redress Mechanisms

Serbian legislation does not support collective redress mechanisms in relation to privacy and data protection. Serbian Consumer Protection Law is a single piece of legislation which provides a collective redress mechanism but only for consumer-related matters. Registered consumer associations and the Ministry of Trade may initiate proceedings for the protection of the consumer's collective interest. However, this mechanism is not available for privacy litigations.

As Serbia is in the process of EU accession, it should take into account the European Union's Representative Actions Directive (EU) 2020/1828 and introduce a collective redress mechanism into other areas of law apart from consumer protection. However, there is no indication that such legislation will be adopted in the near future.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Serbia does not have a comprehensive legal framework governing non-personal data, data sharing, or IoT comparable to the EU Data Act.

3.2 Interaction of Data Regulation and Data Protection

As stated in 1.1 Overview of Data and Privacy-Related Laws and 3.1 Objectives and Scope of Data Regulation, Serbia does not have a special legislation governing non-personal data. In principle, if datasets contain both personal and non-personal data, the PDPA applies to the personal data component. IP rights, trade secrets, and confidentiality obligations govern non-personal data. Organisations should ensure lawful separation, anonymisation, or access controls to avoid the unlawful processing of personal data.

3.3 Rights and Obligations Under Applicable Data Regulation

There are no general statutory rights relating to data access, portability, or interoperability for non-personal data. Such rights arise only contractually.

3.4 Regulators and Enforcement

No dedicated authority oversees non-personal data regulation.

4. Sectoral Topics

4.1 Use of Cookies

Serbian legislation does not have special rules governing the application of cookies, beacons, the use of tracking technologies or behavioural advertising; therefore, the general rules of the PDPA apply to these areas as well.

In practice, opt-in consent is required for non-essential cookies, particularly where personal data is involved.

4.2 Personalised Advertising and Other Online Marketing Practices

The PDPA does not contain special provisions regarding online marketing. However, it does regulate processing for direct marketing purposes and entitles the data subject to object at any time to the processing of personal data concerning them for such marketing, which also includes profiling (Article 37 of the PDPA). With respect to other aspects of online marketing, the general rules on data processing apply.

The Advertising Act (AA) also contains a provision that allows direct advertising only with the prior consent of the person to whom the advertising is sent (Articles 62 and 63 of the AA). Behavioural advertising and targeted advertising are not regulated explicitly by Serbian law.

4.3 Employment Privacy Law

Under the PDPA, the processing of employees' personal data must be carried out in accordance with the provisions of employment law and collective agreements, based on the principles set out by the PDPA. The PDPA also recognises that employment regulations and collective agreements may contain provisions related to the protection of personal data of employees, in which case they also need to specify suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights (Article 91 of the PDPA).

Under the Employment Act of the Republic of Serbia, employers are allowed to collect data regarding their employees where this is prescribed by that Law and other laws related to employment matters. The Employment Act also authorises employers to monitor the work of their employees, a provision that is frequently used in practice as a ground for accessing employees' computers and email communications. In this respect, the Commissioner has taken the position that such access is allowed if the computer and email account were provided by the employer for the purpose of work performance and if it does not invade the employees' privacy. If an employee is using a private email account or private computer, the employer may access the data contained therein only in the presence of that employee, who will then be able to prevent the employer's access to private communication and files. In a recent ruling, the Commissioner took the position that an employer must not continue to use its former employee's email account upon termination of employment, as it contains the employee's name: a piece of personal data whose processing is no longer justifiable, legal and necessary.

4.4 Data Protection in M&A

During the due diligence procedure, the seller should minimise data exposure and use anonymised or pseudonymised data where possible. NDAs must also be signed.

The transfer of personal data in M&A and asset deals is regulated by the PDPA. When they involve personal data (eg, customer or employee databases), the transfer must have a valid legal basis under the LPDP: (i) legitimate interest (Article 12 of the PDPA), (ii) consent if the transaction involves sensitive data or when no other legal basis is available (Article 15), and (iii) legal obligation (Article 17) (eg, employment records).

Once the transaction is closed, the buyer becomes the new data controller and must inform data subjects (customers, employees) of the change. If the transfer changes the purpose of data processing, additional consent may be required. If the buyer is outside Serbia, data transfers must comply with the PDPA's rules on international transfers (transfers to countries without an adequate level of protection require standard contractual clauses (SCCs) or other safeguards.) The

buyer must provide information on how their data will be used post-transfer.

5. International Considerations

5.1 Restrictions on International Data Transfers

Under the PDPA, international transfers of data to a country, a territory or one or more specified sectors within that country, or an international organisation that ensures an adequate level of protection does not require any prior authorisation (Articles 63 and 64 of the PDPA).

It is assumed that an adequate level of protection exists in:

- countries and international organisations that are parties to the Convention;
- countries and international organisations that are considered by the EU to ensure adequate levels of protection of personal data; and
- countries with which the Republic of Serbia has concluded international treaties regarding the transfer of personal data (Article 64 of the PDPA).

The Serbian government has rendered a decision establishing the list of countries, parts of their territory or one or more specified sectors within those countries or international organisations which are considered to ensure the adequate level of personal data protection, specifying the countries to which the transfer of data may occur freely.

Furthermore, under the PDPA, the transfer of personal data is also permitted to a country, a territory of, or one or more specified sectors within, that country, or an international organisation that does not have an adequate level of protection, if the controller or processor provides appropriate safeguards, and if enforceable data subject rights and effective legal remedies for data subjects are available in that country, a territory of, or one or more specified sectors within, that country, or the relevant international organisation (Article 65 of the PDPA).

The appropriate safeguards may be provided by a controller without requiring any specific authorisation from the Data Protection Commissioner by:

- a legally binding instrument between public authorities or bodies;
- standard data protection clauses prepared by the Data Protection Commissioner that regulate the legal relationship between the controller and processor;
- binding corporate rules that regulate processing of personal data by a controller and the group of companies to which the controller belongs;
- an approved code of conduct, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certificate issued in accordance with the PDPA, together with binding and enforceable commitments on the part of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

The appropriate safeguards may also be provided through contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation, or through provisions inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights, but only with the specific authorisation of the Commissioner, which is obliged to give such an authorisation within 60 days from the day of receipt of the request for authorisation (Article 65 of the PDPA).

Further, under the PDPA, the data controller may introduce binding corporate rules that are adhered to by a controller or processor established in the territory of the Republic of Serbia for the purpose of a transfer, or a set of transfers, of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. If the Data Protection Commissioner approves the binding corporate rules, it is considered that a controller has provided adequate

safeguards and that data may be transferred outside of the territory of the Republic of Serbia (Article 67 of the PDPA).

Nonetheless, each international transfer of data has to be lawful – ie, it must be based on one of the legal grounds prescribed by the law:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- it is necessary for compliance with a legal obligation to which the controller is subject;
- it is necessary in order to protect the vital interests of the data subject or of another natural person;
- it is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller; and
- it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by those interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child.

5.2 Government Notifications and Approvals

Under the PDPA, prior approval of the Data Protection Commissioner may be required if data is to be transferred to a country that does not ensure an adequate level of protection (Article 65 of the PDPA). For more details, see **5.1 Restrictions on International Data Transfers**.

5.3 Data Localisation Requirements

Under the current Serbian legislation, there is no requirement for data localisation. However, each instance of data processing, including the transfer of data, has to be made on one of the grounds for data processing stipulated by the PDPA and must ensure adequate levels of data protection (Articles 12 and 65 of the PDPA).

5.4 Blocking Statutes

As stated in **5.1 Restrictions on International Data Transfers**, the transfer of personal data to a country that is not a party to the Convention is subject to prior approval of the Commissioner. If that approval is denied, the data cannot be transferred.

As regards requests for transfer of personal data to a foreign country for the purpose of conducting criminal or civil proceedings, all such requests are governed by the rules of the international treaties and bilateral agreements regulating the co-operation of Serbia with foreign countries in criminal and civil law matters.

5.5 Recent Developments

No major legislative changes occurred in the past year. Future developments are expected in the context of EU accession, AI regulation, and cross-border data governance.

Trends and Developments

Contributed by:

Vladimir Djerić, Lena Petrovic and Katarina Radovic
Mikijelj, Janković & Bogdanović

Mikijelj, Janković & Bogdanović is a Belgrade-based law firm established in 1985, with a long-standing practice in dispute resolution, intellectual property, and regulatory matters. The firm's data protection and privacy work is handled by a dedicated team of three lawyers, including two partners and a senior associate. The team advises domestic and international clients on compliance with the Serbian Personal Data Protection Act, cross-border data transfers, data breach response, employment-related data process-

ing, and privacy issues arising in media, advertising, and digital services. The firm has experience advising clients operating in the telecommunications, pharmaceuticals, online commerce, gambling, and media sectors. The data protection practice works closely with the firm's dispute resolution, employment, IP, and corporate teams, allowing it to address data protection issues arising in regulatory proceedings, commercial transactions, and litigation.

Authors



Vladimir Djerić is a partner at Mikijelj, Janković & Bogdanović. He advises clients on dispute resolution, media law, data protection and privacy.

Vladimir represents clients in court disputes involving privacy,

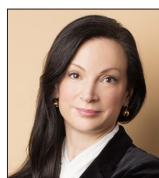
defamation, and freedom of expression. His practice includes advising media organisations, technology companies, and regulated businesses on compliance and litigation risk related to personal data processing. He is a member of the Belgrade Bar Association.



Lena Petrovic is a senior associate at Mikijelj, Janković & Bogdanović. She advises clients on data protection and privacy, advertising law, dispute resolution, media law and intellectual property. Lena works on GDPR-

aligned compliance under Serbian law, international data transfers, direct marketing practices, and

privacy issues arising in digital and media projects. She assists clients in regulatory proceedings and litigation involving personal data protection. She also represents clients in proceedings before the Commissioner for Information of Public Importance and Protection of Personal Data. Lena is a member of the Belgrade Bar Association.



Katarina Radovic is a partner at Mikijelj, Janković & Bogdanović. Her practice focuses on employment law, data protection, dispute resolution, and intellectual property. Katarina advises employers on the lawful

processing of employee data, workplace monitoring, internal investigations, and data protection compliance in HR-related processes. She has experience representing clients in administrative and court proceedings concerning personal data protection and employment disputes. Katarina is a member of the Belgrade Bar Association.

Mikijelj, Janković & Bogdanović

Vlajkovicева 28
11000 Belgrade
Serbia

Tel: +381 11 3231 970
Fax: +381 11 3245 065
Email: office@mjb.rs
Web: www.mjb.rs



Introduction

While the legislative framework has remained formally unchanged since the entry into force of the Law on Personal Data Protection in 2019, the Commissioner for Information of Public Importance and Personal Data Protection (the “Commissioner”) has continued to develop a rich and increasingly detailed body of supervisory and complaints practice. This practice now provides meaningful guidance on how the core principles of Serbian data protection law are to be interpreted and applied in concrete situations.

The Commissioner’s latest annual publication, issued in early 2026 and covering cases resolved during 2025, illustrates a clear shift away from abstract discussions of compliance towards a highly fact-specific and outcome-oriented approach. The focus is no longer on whether controllers are formally aware of their obligations, but on whether they can demonstrate accountability, proportionality and necessity in practice.

At the same time, the Commissioner has publicly acknowledged that work on a new Law on Personal Data Protection is well advanced. This legislative activity, although not yet completed, provides important context for understanding current enforcement trends: supervisory practice in 2025 increasingly anticipates stricter standards for emerging technologies, digital services and large-scale processing operations.

Accountability as a Central Enforcement Benchmark

From formal compliance to demonstrable compliance

One of the most significant trends observed in 2025 is the Commissioner’s insistence on demonstrable accountability. Controllers are no longer assessed primarily on the basis of whether they invoke a recognised legal basis or cite relevant statutory provisions. Instead, they are expected to show that compliance considerations were embedded into decision-making processes before processing commenced.

Across a wide range of cases, the Commissioner criticised controllers for failing to produce internal documentation explaining why a particular processing operation was necessary, proportionate and law-

ful. This was particularly evident in cases involving reliance on legitimate interest as a legal basis. Controllers were repeatedly unable to provide evidence of a prior balancing test or risk assessment, leading the Commissioner to conclude that legitimate interest had been invoked retroactively rather than as part of a structured compliance process.

Consequences of inadequate documentation

The absence of documentation was not treated as a purely procedural shortcoming. Instead, it was directly linked to substantive violations of the principles of lawfulness, transparency and accountability. In several cases, the Commissioner explicitly stated that the failure to document assessments undermined the credibility of the controller’s arguments and prevented a meaningful review of whether less intrusive alternatives had been considered.

This approach aligns Serbian supervisory practice more closely with EU enforcement standards, where accountability is understood as an active and ongoing obligation rather than a formalistic requirement.

Employee Data and Workplace Monitoring

GPS tracking and continuous monitoring

Employee data processing remained a key enforcement priority in 2025, with particular emphasis on monitoring technologies. Several high-profile cases concerned the use of GPS systems in company vehicles, ostensibly for purposes such as asset protection, traffic safety and operational efficiency.

The Commissioner consistently held that continuous GPS monitoring represents a serious interference with employees’ right to privacy, as it enables real-time tracking of movement and behaviour. While acknowledging that asset protection may constitute a legitimate interest in principle, the Commissioner rejected blanket or speculative justifications. Controllers were expected to demonstrate actual risks, such as documented incidents of theft or misuse, and to explain why less intrusive measures would not achieve the same objectives.

Legitimate interest and the employment context

A recurring theme in these decisions was the inherent imbalance of power in employment relationships.

The Commissioner reiterated that employee consent is rarely valid and that legitimate interest requires particularly careful assessment in the workplace context. Where controllers failed to demonstrate that employee interests and rights had been adequately weighed, processing was found to be unlawful.

Notably, in at least one case, the Commissioner concluded that the only possible legal basis for the proposed processing would be valid, freely given consent, while simultaneously highlighting the difficulty of obtaining such consent in practice. This tension illustrates the narrow space available for intrusive monitoring measures under Serbian law.

Data Breaches Arising From Routine Communications

Email disclosures as reportable breaches

Another prominent enforcement trend in 2025 concerned personal data breaches resulting from routine electronic communications. The Commissioner addressed multiple cases in which controllers disclosed email addresses of large numbers of individuals by sending group messages without using blind carbon copy (BCC) functionality.

In these cases, the Commissioner treated the disclosure of email addresses as a breach of confidentiality and integrity, regardless of whether sensitive data was involved. Importantly, the Commissioner emphasised that the absence of complaints from affected individuals does not negate the existence of a breach or the controller's reporting obligations.

Failure to notify and organisational shortcomings

Controllers were criticised not only for the initial disclosure, but also for failing to recognise the incident as a personal data breach requiring notification. The Commissioner highlighted deficiencies in internal incident response procedures, staff training and awareness.

These decisions demonstrate that basic operational practices, such as email communication, are now firmly within the scope of enforcement scrutiny. Public authorities, educational institutions and other organisations handling large mailing lists are expected to

have clear internal rules governing electronic communications.

Protection of Children's Personal Data

Online publication of photographs

The protection of minors' data was another area of heightened enforcement activity. In several cases, the Commissioner examined the publication of photographs of children on websites operated by private entities, including commercial service providers and event organisers.

The Commissioner adopted a strict interpretation of applicable standards, holding that the online availability of children's images constitutes processing that requires a clear legal basis and, in most cases, informed parental consent. The use of watermarks or technical limitations on image quality was deemed insufficient to mitigate the risks associated with public accessibility.

Data protection impact assessments and organisational duties

In addition to consent-related issues, the Commissioner criticised controllers for failing to conduct data protection impact assessments and for not appointing data protection officers where required. The absence of contractual arrangements with event organisers or other partners was also highlighted as a compliance failure.

These cases illustrate an increasingly holistic enforcement approach, in which the legality of processing is assessed in the context of the entire organisational and contractual framework, rather than in isolation.

Data Minimisation and Public Transparency

Publication of recruitment and appointment documents

A further important trend in 2025 concerned the application of data minimisation principles in the context of public transparency. The Commissioner addressed multiple cases involving the publication of recruitment decisions and ranking lists containing personal identification numbers and home addresses of candidates.

Controllers frequently argued that such disclosures were justified by transparency obligations or by the

consent of candidates. The Commissioner rejected these arguments, emphasising that transparency does not require the publication of all personal data contained in official documents.

Rejection of consent as a legal basis

In line with earlier practice, the Commissioner reiterated that consent is generally not an appropriate legal basis in recruitment and employment contexts. Candidates are typically in a position of dependency, and consent obtained as a condition of participation in a procedure cannot be considered freely given.

This reinforces a broader enforcement message: controllers must design transparency mechanisms that respect data protection principles, rather than attempting to justify excessive disclosure through consent.

Security Measures and Organisational Compliance *Technical and organisational measures*

Across multiple enforcement areas, the Commissioner placed strong emphasis on the obligation to implement appropriate technical and organisational measures. Failures to anonymise documents, restrict access or establish clear retention periods were repeatedly identified as violations.

The Commissioner noted that security obligations are dynamic and context-dependent. Measures that may have been acceptable in smaller-scale or analogue environments are no longer sufficient in digital and networked contexts.

Staff awareness and internal policies

Several decisions highlighted the absence of internal policies or the failure to implement existing ones effectively. Controllers were criticised for treating compliance as a one-time exercise rather than an ongoing organisational responsibility.

This trend suggests that future enforcement will increasingly focus on governance structures, training programmes and internal controls, rather than isolated technical failures.

Procedural Developments and Remedies

Use of warnings and corrective measures

During 2025, the Commissioner continued to rely primarily on corrective measures, such as warnings, orders to delete data and instructions to align processing with legal requirements. Monetary penalties remained relatively rare, reflecting a continued emphasis on corrective rather than punitive enforcement.

However, the detailed reasoning provided in decisions indicates a readiness to escalate enforcement where non-compliance persists or where risks to individuals are particularly high.

Interaction with complaints procedures

In complaints-based proceedings, the Commissioner further clarified the scope and limits of data subject rights, particularly in relation to erasure and access. Several decisions confirmed that data cannot be erased where retention is required by law or necessary for the achievement of legitimate processing purposes.

Legislative Outlook and Future Priorities

Towards a new Law on Personal Data Protection

In the introductory part of the 2026 publication, the Commissioner confirmed that work on a new Law on Personal Data Protection had progressed significantly during 2025, raising expectations of imminent legislative reform.

Although details of the proposed amendments have not yet been made public, the Commissioner indicated that the new law aims to be clearer, more precise and better adapted to contemporary technological realities, including AI and advanced digital systems.

Anticipated impact on enforcement

Given current supervisory trends, it is likely that future enforcement will place even greater emphasis on proactive compliance, risk assessment and governance. Controllers operating in Serbia should therefore view 2025 enforcement practice not merely as retrospective guidance, but as an indication of the standards that will be expected under the forthcoming legal framework.

Conclusion

Key trends include a strong emphasis on accountability, strict scrutiny of employee monitoring, heightened sensitivity to children's data, and a firm application of data minimisation principles even in areas traditionally associated with transparency. As legislative reform approaches, these developments provide valuable insight into the direction of Serbian data protection law and the expectations placed on controllers in the years ahead.

SINGAPORE

Law and Practice

Contributed by:

Chong Kin Lim, David N. Alfred and Anastasia Chen

Drew & Napier LLC



Contents

1. Legal and Regulatory Framework p.411

- 1.1 Overview of Data and Privacy-Related Laws p.411
- 1.2 Rights and Obligations p.412
- 1.3 Special Categories of Personal Data p.414
- 1.4 Processing of Personal Data for Research and Development Purposes p.415
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.416
- 1.6 Data Breach Requirement p.417
- 1.7 Regulators p.418
- 1.8 Enforcement Proceedings and Fines p.418
- 1.9 Enforcement Trends p.420

2. Privacy Litigation p.420

- 2.1 Privacy Litigation Overview p.420
- 2.2 Recent Case Law p.421
- 2.3 Collective Redress Mechanisms p.421

3. Requirements for the Protection and Processing of Non-Personal Data p.421

- 3.1 Objectives and Scope of Data Regulation p.421
- 3.2 Interaction of Data Regulation and Data Protection p.422
- 3.3 Rights and Obligations Under Applicable Data Regulation p.422
- 3.4 Regulators and Enforcement p.422

4. Sectoral Topics p.422

- 4.1 Use of Cookies p.422
- 4.2 Personalised Advertising and Other Online Marketing Practices p.423
- 4.3 Employment Privacy Law p.423
- 4.4 Data Protection in M&A p.423

5. International Considerations p.424

- 5.1 Restrictions on International Data Transfers p.424
- 5.2 Government Notifications and Approvals p.425
- 5.3 Data Localisation Requirements p.425
- 5.4 Blocking Statutes p.425
- 5.5 Recent Developments p.425

Drew & Napier LLC established a dedicated Data Protection, Privacy and Cybersecurity Practice to leverage its unrivalled experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. The firm represents many regional companies, multinationals, industry associations, government bodies and regulators, and regularly assists them on a wide range of matters in Singapore and ASEAN member countries.

At the forefront of data protection law in Singapore since 2013, the Data Protection, Privacy & Cybersecurity Practice Group has worked on significant data protection enforcement cases and appeals, including those involving cybersecurity elements. Building on its experience in this field, the Drew Data Protection & Cybersecurity Academy was established in 2020 to offer clients services relating to data protection and cybersecurity compliance, including training, consulting and external data protection officer services.

Authors



Chong Kin Lim heads Drew & Napier's highly regarded TMT practice group. His clients include telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.

Chong Kin has worked on every significant development in the Singapore TMT market, and continues to play a key role in the development of sectoral competition regulation in Singapore. He was the lead external counsel in the liberalisation of the telecommunications, media and postal sectors, and has assisted regulators in conceptualising and drafting "first-of-its-kind" sectoral competition legislation and frameworks.



David N. Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy & Cybersecurity Practice Group. He is concurrently co-head and programme director of the Drew Data Protection &

Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 25 years' experience advising on a broad range of matters relating to digital technology, telecommunications and the internet. He has substantial experience advising on data protection and cybersecurity compliance, regulatory enforcement, data breaches and international aspects of data protection. Prior to joining the firm, David was the first Chief Counsel of Singapore's data protection authority, the Personal Data Protection Commission.



Anastasia Chen is a director of Drew & Napier LLC and deputy head of the firm's Data Protection, Privacy & Cybersecurity Practice Group. Prior to joining the firm, Anastasia was Deputy Chief Counsel to Singapore's

Personal Data Protection Commission (PDPC) and Info-communications Media Development Authority (IMDA) for over nine years, during which she served as lead counsel for PDPC's matters, IMDA's procurement and intellectual property portfolios, as well as IMDA's Data Administration Group. She has received accolades from legal publications, with clients commending her deep industry and regulatory expertise, as well as legal acumen, especially when dealing with novel problems.

Drew & Napier LLC

10 Collyer Quay
10th Floor
Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Fax: +65 6535 4864
Email: mail@drewnapier.com
Web: www.drewnapier.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Singapore's data protection framework is laid out in the Personal Data Protection Act 2012 (PDPA), which is the main statute governing the collection, use, disclosure and care of personal data in the private sector. Oversight, administration and enforcement of the PDPA are vested in the Personal Data Protection Commission (PDPC).

The core data protection obligations are set out in Parts 3 to 6A of the PDPA. These provisions regulate, among other matters, the collection, use, disclosure, access, correction, accuracy security, retention, overseas transfer of personal data and notification of data breaches (collectively, the "Data Protection Provisions"). In addition, Parts 9 and 9A of the PDPA establish Singapore's national Do Not Call (DNC) Registry, and set out the duties imposed on organisations in relation to the transmission of specified marketing communications to Singapore telephone numbers.

The PDPA was updated through the Personal Data Protection (Amendment) Act 2020. The majority of the significant amendments, including mandatory data breach notifications and new consent-related provisions, took effect on 1 February 2021.

The PDPA has both territorial and extraterritorial effect, applying to all organisations that are not a public agency, whether or not formed or recognised under

the laws of Singapore, or resident or having an office or a place of business in Singapore.

The PDPA is supplemented by subsidiary regulations, including the following:

- Personal Data Protection Regulations 2021 (the "PDP Regulations"), which address matters such as data transfers out of Singapore and procedures relating to access and correction requests;
- Personal Data Protection (Enforcement) Regulations 2021 (the "Enforcement Regulations"), which govern enforcement processes and powers;
- Personal Data Protection (Notification of Data Breaches) Regulations 2021, which prescribe thresholds and timelines for mandatory breach notification;
- Personal Data Protection (Composition of Offences) Regulations 2021;
- Personal Data Protection (Appeal) Regulations 2021; and
- Personal Data Protection (Do Not Call Registry) Regulations 2013.

These regulations are legally binding and are issued pursuant to the PDPA.

The PDPA operates alongside sectoral laws and regulations that set out further data protection and cybersecurity obligations for the compliance of regulated entities. Some examples include:

- Healthcare Services Act 2020 (No 3 of 2020) (HCSA), addressing the confidentiality and retention of medical records;
- Code of Practice for Competition in the Provision of Telecommunication Services 2012 issued under the Telecommunications Act 1999 (2020 Revised Edition), regulating how telecommunications licensees may handle end-user service information; and
- Banking Act 1970 (2020 Revised Edition), containing statutory banking secrecy obligations governing the disclosure and handling of customer information by banks.

Additionally, the PDPC has issued a substantial body of advisory guidelines. While these guidelines are not legally binding, they play an important interpretive role by explaining how the PDPC understands and applies the PDPA in practice, and they are frequently relied upon by organisations seeking compliance certainty.

See 3.1 Objectives and Scope of Data Regulation and 1.5 Processing of Personal Data in the Context of Artificial Intelligence on how the PDPA interacts with laws governing non-personal data and AI respectively.

1.2 Rights and Obligations

Primary Obligations

The PDPA generally imposes 11 primary obligations on organisations.

Consent obligation

Generally, an organisation may not collect, use or disclose personal data unless the individual has given consent or is deemed to have consented under the PDPA. However, consent is not required where the collection, use or disclosure is authorised or mandated by written law.

The PDPA recognises a number of exceptions where personal data may be processed without consent. These include situations involving:

- the protection of vital interests;
- matters of public interest;
- an organisation's legitimate interests;
- business asset transactions;
- business improvement purposes; and

- research.

Purpose limitation obligation

Personal data may only be collected, used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances. Where required under the PDPA, those purposes must also be made known to the individual.

Notification obligation

Organisations are generally required to inform individuals of the purposes for which their personal data is being collected, used or disclosed. Notification is not necessary where consent is deemed by conduct or contractual necessity in accordance with the PDPA or where processing without consent is permitted pursuant to an exception to consent under the PDPA (save that there are disclosure/notification requirements when relying on the exceptions relating to general legitimate interests and managing employees).

Access obligation

Upon request, an organisation must provide an individual with access to their personal data in the organisation's possession or control, as well as information about how that data has been used or disclosed. The obligation is subject to exceptions set out in the Fifth Schedule to the PDPA, including circumstances where disclosure would compromise an ongoing investigation. There are also specific circumstances where access is prohibited. Further details are set out under "Data Subject Rights" below.

Correction obligation

Organisations must, on request, correct inaccuracies or omissions in an individual's personal data, unless there are reasonable grounds for refusing the correction or the request falls within one of the prescribed exceptions in the Sixth Schedule to the PDPA. Further details are set out under "Data Subject Rights" below.

Accuracy obligation

Where personal data is likely to be used to make a decision affecting an individual, or disclosed to another organisation, reasonable steps must be taken to ensure that the data is accurate and complete. This obligation is context-specific and turns on what is reasonable in the circumstances.

Protection obligation

Organisations are required to implement reasonable security arrangements to safeguard personal data in their possession or under their control. These measures must protect against unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Retention limitation obligation

Personal data must not be retained for longer than is necessary to fulfil the purposes for which it was collected. Once those purposes are no longer served, and retention is no longer required for legal or business reasons, the data must be deleted or anonymised.

Transfer limitation obligation

An organisation may only transfer personal data outside Singapore if it ensures that the recipient jurisdiction provides a level of protection comparable to that under the PDPA.

Data breach notification obligation

In the event of a data breach, an organisation must conduct an assessment to determine whether the breach is notifiable under the PDPA. Where notification is required, the organisation must notify the Personal Data Protection Commission (PDPC) as soon as practicable and, in any event, no later than three calendar days after making the assessment. In specified cases, affected individuals must also be informed.

Accountability obligation

Finally, organisations must be able to demonstrate compliance with the PDPA. This includes appointing a data protection officer, developing and implementing internal data protection policies and practices, and embedding data protection considerations into organisational governance and operations.

Data Subject Rights

The PDPA confers a limited set of rights on individuals in relation to their personal data. These rights include the ability to withdraw consent to data processing, to request access to personal data held by organisations, and to seek the correction of inaccuracies or omissions in such data.

Right of access to personal data

Under Section 21 of the PDPA, individuals have the right to request access to personal data about them that is in the possession or under the control of an organisation, as well as information about how that data has been used or disclosed within the preceding year. However, access is prohibited under the following circumstances pursuant to Section 21 (3) of the PDPA:

- threaten the safety or health of another individual;
- cause immediate or grave harm to the safety or health of another individual;
- reveal another individual's personal data;
- disclose the identity of an individual who provided personal data, without that individual's consent; or
- be contrary to national interest.

Furthermore, an organisation is not obliged to provide access to an individual's personal data or related information where the request falls within the situations set out in the Fifth Schedule to the PDPA.

Right to correction

Under Section 22 of the PDPA, individuals may request the correction of errors or omissions in their personal data. Where a correction is made, the organisation is generally required to send the corrected data to other organisations to which it was disclosed within the preceding year, unless this is unnecessary for legal or business purposes. The correction right does not extend to opinion data or derived personal data, and is subject to exceptions set out in the Sixth Schedule to the PDPA.

Right to withdraw consent

Under Section 16 of the PDPA, individuals may, upon giving reasonable notice, withdraw any consent (including deemed consent) previously given for the collection, use or disclosure of their personal data. Following withdrawal, the organisation must cease the relevant processing activity unless continued processing without consent is authorised or required under the PDPA or other written law.

Right to object to marketing

See detail set out under "Right to withdraw consent".

Individuals may also object to the receipt of specified marketing messages by registering their Singapore telephone numbers with one or more of the national DNC Registers. Registration restricts the sending of telemarketing messages to those numbers, unless clear and unambiguous consent to the sending of the telemarketing message is obtained in evidential form.

Right to lodge complaints

Individuals may lodge complaints with the PDPC in respect of alleged breaches of the PDPA. The PDPC may facilitate resolution, refer the matter for mediation, or conduct a formal investigation and take enforcement action where appropriate.

Main Compliance Requirements for Organisations

The following are the main compliance requirements.

Establish data protection governance

- Appoint a Data Protection Officer (DPO) and make the DPO's business contact details publicly available.
- Adopt and maintain written data protection policies and documented practices/processes to ensure the organisation complies with the PDPA.

Understand and manage personal data holdings

- Identify and document personal data assets and data flows across the organisation.
- Assess key data protection risks and compliance gaps (including in existing systems and processes).

Implement basic operational controls

- Put in place procedures for handling access, correction and consent withdrawal requests.
- Implement reasonable technical and organisational security measures to protect personal data.
- Establish retention and disposal practices to prevent unnecessary retention of personal data.

Prepare for data breaches and complaints

- Establish a data breach response plan and designate a response team.
- Implement internal escalation and assessment procedures for suspected data breaches.
- Put in place a basic complaint-handling process for data protection matters.

Train staff and raise awareness

- Provide periodic training to employees who handle personal data.
- Communicate internal policies and expectations relating to personal data protection.

Review and maintain compliance

- Conduct periodic reviews of data protection policies and practices.
- Test breach response readiness (eg, through table-top exercises).
- Consider data protection impact assessments for new or significantly changed systems or uses of data.

1.3 Special Categories of Personal Data Processing of Health Data

The PDPA does not designate health data as a separate statutory category of "special" personal data. However, health and medical information is generally regarded as particularly sensitive, and its processing is subject to heightened expectations under the PDPA, as supplemented by sector-specific guidance and legislation.

The collection, use and disclosure of health data are governed primarily by the general PDPA obligations. PDPC has issued the Advisory Guidelines for the Healthcare Sector (Revised 20 September 2023), which provide practical guidance on how these obligations apply in common healthcare scenarios. The guidelines address, among other matters:

- the role of consent in clinical care;
- circumstances where processing without consent may be permitted; and
- the handling of access and correction requests relating to medical records.

Organisations handling health data are expected to implement stronger security and access controls, reflecting the sensitivity of such data, and to ensure that collection and use are limited to what is reasonably necessary for healthcare or related purposes. Retention of medical records must also be justified by ongoing care needs, legal requirements or professional standards.

In addition to the PDPA, healthcare providers are subject to sector-specific statutory requirements. The HCSA, the Healthcare Services (General) Regulations 2021, and applicable licensing conditions impose obligations relating to patient confidentiality and record-keeping, which operate alongside the PDPA framework.

Processing of Data Relating to Minors

The processing of minors' personal data is governed by the Data Protection Provisions, as supplemented by guidance issued by the PDPC.

The principal requirement concerns consent. Whether a minor may validly consent depends on whether the minor has sufficient understanding of the nature and consequences of the collection, use or disclosure of personal data. The PDPC has indicated that, as a general benchmark, minors aged 13 years and above are typically capable of providing valid consent on their own behalf. Where an organisation has reason to believe that a minor lacks such understanding, consent must be obtained from a parent or legal guardian.

For online products or services likely to be accessed by children (individuals below 18 years of age), the PDPC's Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment impose additional expectations. In particular, organisations must ensure that privacy notices and consent mechanisms are age-appropriate and readily understandable, and that children aged between 13 and 17 years understand the consequences of giving and withdrawing consent.

Children's personal data is generally regarded by the PDPC as sensitive, necessitating stronger protection. The use of such data or profiles to target harmful or inappropriate content (as defined in the Code of Practice for Online Safety, issued under the Broadcasting Act 1994) is considered unreasonable. Organisations are also expected to implement enhanced safeguards and to assess data protection risks, such as through data protection impact assessments, where products or services are likely to involve children's data.

Processing of Data Relating to Criminal Convictions and Investigations

The processing of personal data relating to criminal convictions and investigations is subject to the Data Protection Provisions. Under the PDPA, processing data without consent is permitted where it is necessary for purposes such as:

- investigations or proceedings;
- compliance with written law; or
- where required by public authorities exercising lawful functions.

Further, where an organisation has provided personal data to a prescribed law enforcement authority without the individual's consent, the PDPA requires the organisation to refrain from notifying the individual of that disclosure. Personal data gathered in connection with investigations, prosecutions or related proceedings may fall outside the access regime under the PDPA, particularly while proceedings remain pending. In such circumstances, access to the data should generally be pursued through the relevant criminal or civil discovery processes, which operate independently of the PDPA framework.

1.4 Processing of Personal Data for Research and Development Purposes

Generally, the PDPC promotes the use of anonymisation as a means of tapping on data for insights where individuals need not be identified.

In Singapore, the PDPC defines anonymisation as the process of "converting personal data into data that cannot identify any particular individual". A dataset would be considered anonymised, where there is no serious possibility that an individual can be identified from the dataset when it is combined with other information that the data recipient has or is likely to have access to, by carrying out an assessment of the risk of re-identification. The following factors go towards lowering re-identification risks:

- the intended use of the anonymised data and the extent of its disclosure are controlled, for example where the data is used internally or disclosed only to a restricted group of recipients rather than made publicly available;

- access to the anonymised data is limited to recipients who do not possess special knowledge of the individuals concerned, or who do not have access to complementary information that could reasonably be used to re-identify individuals;
- the recipient does not have both the ability and motivation to re-identify individuals from the dataset, or where such risks are mitigated through appropriate legal or regulatory safeguards; or
- the anonymised dataset can reasonably be expected to remain anonymised over time, having regard to foreseeable technological developments, data availability and data-linking techniques.

However, where the nature of data is highly sensitive to individuals (eg, records of individuals with HIV), even if the organisation assesses that there is a less than serious possibility of an individual being re-identified from the data, PDPC has cautioned organisations to carefully consider whether using or disclosing such data would be appropriate.

Once data is anonymised, such that individuals can no longer be identified, it no longer falls under the PDPA. Therefore, this could allow medical device or software providers to use such anonymised data for research and development without patient consent. Organisations should note that, if the risk of re-identification is more than a serious possibility, the data is brought back under the Data Protection Provisions, such as obtaining consent subject to approved exceptions.

Impact of the European Health Data Space Regulation (EHDS)

The EHDS regime is designed to govern entities operating within the EU health data ecosystem, and its core obligations apply mainly to health data holders established in the EU. Singapore-based companies may be directly subject to the EHDS if they have an established presence within the EU, and where they fall within the definition of a health data holder as entities developing health-related products or services, and wellness applications, or conducting healthcare-related research – and, in that capacity, either process personal electronic health data as a controller or have the ability to make non-personal electronic health data available through control of the relevant technical systems.

Singapore life sciences companies may also be indirectly affected where they operate EU subsidiaries, collaborate with EU healthcare providers or research institutions, or supply digital health products, medical devices or Electronic Health Record (EHR)-linked services into the EU market. In such cases, EU-based affiliates or partners may be required to comply with EHDS obligations on data access, secondary use and secure processing, which can flow down contractually to Singapore parent entities or vendors. In contrast, Singapore companies seeking to access EU health datasets for research or product development will generally not qualify as health data users under the EHDS unless Singapore is recognised by the EU as offering reciprocal access. However, this has not occurred to date.

Domestically, Singapore parliament has passed the Health Information Bill, which aims to structure national data sharing through the National Electronic Health Record System, mirroring the EHDS.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

There is currently no AI-specific legislation in Singapore. The PDPA applies to the processing of personal data throughout the development, training, testing, deployment and operation of AI systems. While the PDPA does not contain provisions specifically tailored to AI, organisations deploying AI systems that collect, use or disclose personal data must comply with all obligations in the PDPA, such as the consent (Sections 13 to 20 of the PDPA), notification (Section 20 of the PDPA) and accountability (Sections 11 and 12 of the PDPA) obligations.

On 1 March 2024, the PDPC issued the Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems, which articulate a risk-based approach to AI governance and provide targeted guidance on how the PDPA applies in AI contexts. These guidelines emphasise that consent and notification obligations must operate together to ensure that individuals are meaningfully informed when their personal data is used in AI-driven features or automated decision-making.

Organisations are expected, where practicable, to provide a clear explanation of:

- the function of the AI system of the product that utilises personal data;
- a general description of categories of personal data to be collected and processed;
- an explanation on how such data supports or influences the product feature; and
- the specific data features likely to affect the product feature.

Where detailed explanations cannot be provided due to legitimate commercial sensitivity or security concerns, organisations are expected to document and justify such limitations internally.

Under the PDPA's accountability obligation, organisations must implement internal governance measures to ensure that AI-assisted decisions are fair and reasonable. This includes maintaining policies, risk controls and review mechanisms appropriate to the context in which the AI system is used. The degree of transparency and oversight expected is risk-proportionate, taking into account factors such as:

- the potential impact on individuals;
- the sensitivity of the data involved; and
- the extent to which decisions are automated without human involvement.

There are currently no legally prohibited AI use cases or formally designated "high-risk" AI categories under data protection law.

The Info-communications Media Development Authority (IMDA) and the PDPC have jointly issued the Model Artificial Intelligence Governance Framework. It is a voluntary but influential instrument that encourages organisations to align their internal governance, policies and practices with recognised data protection standards, including the PDPA and international principles such as the OECD Privacy Principles.

1.6 Data Breach Requirement

Under the PDPA, a data breach occurs when personal data is accessed, collected, used, disclosed, copied, modified or lost without authorisation, or when there is

a loss of a storage medium containing personal data in circumstances that make such outcomes likely. Organisations must expeditiously determine whether a data breach meets the threshold for notification, generally performing this assessment as soon as possible and typically within 30 days of becoming aware of the incident.

Where a breach is deemed notifiable, the organisation must report it to the PDPC within three days of making that determination. A breach is notifiable if it either (i) causes, or is likely to cause, significant harm to affected individuals, or (ii) affects 500 or more individuals. Once notification to the PDPC has been made, if the breach involves actual or potential significant harm to individuals, organisations are generally required to inform the affected individuals promptly.

The following are practical steps to be taken by organisations when a data breach occurs.

- *Immediate containment* – For example, secure affected systems and data to prevent further unauthorised access.
- *Assessment of risk* – Determine the scope of the breach, the type of personal data involved and the potential harm to individuals.
- *PDPC notification* – If the breach is notifiable, submit a report to the PDPC within three days of determination.
- *Notification of individuals* – Where significant harm is likely or has occurred, communicate with affected individuals in a clear and timely manner.
- *Remediation and prevention* – Address system vulnerabilities, review policies and procedures, and implement measures to reduce the likelihood of recurrence.

If a data processor suspects that a breach has occurred in relation to personal data it handles on behalf of a data controller, it must alert the controller swiftly. The controller is then responsible for evaluating whether the incident meets the notifiable threshold and for co-ordinating any required reporting to the PDPC and affected individuals.

Notifiable breaches may trigger investigations by the PDPC, which has the authority to examine the

organisation's breach response and data protection practices, potentially resulting in enforcement action. In addition, data breaches expose organisations to potential privacy litigation, outlined in **2. Privacy Litigation**.

1.7 Regulators

The PDPC is the primary regulator of the PDPA. Its jurisdiction covers private sector organisations. Its core functions include:

- promoting awareness of data protection in Singapore;
- providing advisory, consultancy and technical services relating to data protection;
- advising the Singapore government on policy and representing Singapore internationally;
- conducting research and educational programmes;
- facilitating technical co-operation and exchange in the area of data protection with other organisations, including foreign data protection authorities and international or intergovernmental organisations, on its own behalf or on behalf of the government; and
- administering and enforcing the PDPA and functions assigned by law or the Minister.

Investigations may arise from complaints or on the PDPC's own initiative. According to the Advisory Guidelines on Enforcement of the Data Protection Provisions, the PDPC would consider factors such as:

- whether the organisation may have breached all or a substantial portion of its obligations under the PDPA;
- whether the organisation's actions reflect a systemic lapse in compliance, including a failure to put in place or maintain adequate internal policies and procedures to ensure adherence to the PDPA;
- the number of individuals who have been, or could potentially be, affected by the organisation's actions;
- the extent of harm or adverse impact suffered by the complainant or any affected individuals;
- whether the organisation has a history of PDPA contraventions or has failed to take adequate remedial steps to prevent a recurrence of earlier breaches;

- whether the complainant had previously sought to resolve the matter directly with the organisation without success;
- where the PDPC has attempted to facilitate dispute resolution, whether the parties agreed to participate, their conduct throughout the process, and the eventual outcome of such resolution efforts;
- where the PDPC has initiated a review, whether the organisation complied with its obligations under the Enforcement Regulations, its conduct during the review, and the result of that review; and
- broader considerations of public interest.

In the course of investigations, the PDPC may:

- compel the production of documents and information;
- compel witnesses, and conduct oral examinations or record statements; and
- enter premises to take necessary equipment or copies of documents (amongst other things).

1.8 Enforcement Proceedings and Fines

The PDPC is responsible for enforcing the PDPA. It is guided by four key objectives as set out in the PDPC's Guide to Active Enforcement (revised on 1 October 2022), namely:

- to respond to PDPA breaches effectively, with attention to incidents affecting large numbers of individuals or involving personal data that may result in significant harm;
- to apply enforcement measures in a manner that is proportionate and consistent across organisations found to be in breach of the PDPA;
- where penalties imposed function as a meaningful deterrent against future non-compliance; and
- to ensure that organisations in breach take adequate remedial action to rectify weaknesses in the protection and handling of personal data within their possession or control.

When a possible personal data incident comes to the PDPC's attention (whether through a complaint, self-report or other means), the PDPC will first assess whether the matter warrants a formal investigation. The Commissioner may decide not to investigate where:

- the issue is more appropriately resolved through facilitation or mediation;
- the facts do not suggest a breach of the data protection obligations; or
- the organisation concerned falls primarily within the remit of another sectoral regulator better placed to address the matter.

If investigation is warranted, the PDPC formally opens a case. During an investigation, the PDPC may:

- issue notices for the production of documents and information from the relevant organisations;
- carry out interviews and record statements from the organisations and individuals concerned; and
- where appropriate, undertake site visits to obtain a comprehensive understanding of the facts.

The organisation under investigation is given the opportunity to respond and make representations before any decision is reached.

After evaluating the facts of the case and representations, the PDPC determines whether a breach has occurred and may issue directions to the organisation. These may include financial penalties, which currently can reach SGD1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher.

When setting financial penalties, the PDPC considers factors such as:

- the nature, gravity and length of the organisation's or individual's non-compliance;
- the type and sensitivity of the personal data affected by the non-compliance;
- whether the organisation or individual derived any financial gain, or avoided a financial loss, as a result of the non-compliance;
- the steps taken by the organisation or individual to reduce or address the impact of the non-compliance, including how promptly and effectively those steps were implemented;
- whether, notwithstanding the non-compliance, the organisation or individual had put in place appropriate and sufficient measures to comply with the PDPA;

- any history of previous non-compliance with the PDPA by the organisation or individual;
- the extent to which the organisation or individual complied with any directions issued under Section 48I or 48L(4) to remedy or mitigate the effects of the non-compliance;
- whether the proposed financial penalty is appropriate and effective in promoting compliance and deterring future breaches of the PDPA;
- the anticipated impact of the financial penalty on the organisation or individual, including their ability to continue normal operations; and
- any other factors considered relevant.

Beyond financial penalties, the PDPC may issue administrative directions to compel compliance, including requiring organisations to cease unlawful data practices, correct or delete personal data, or provide access to affected individuals, with such directions enforceable through the courts. Separately, the PDPA also recognises a private right of action for individuals who suffer loss or damage.

An organisation or individual dissatisfied with a direction or decision of the PDPC may first apply to the PDPC for reconsideration, under Section 48N of the PDPA. Following a reconsideration decision, the aggrieved party may appeal to the Data Protection Appeal Panel pursuant to Section 48Q of the PDPA. Alternatively, an appeal may be brought directly to the Appeal Panel without first seeking reconsideration.

A further appeal from a decision of the Appeal Panel lies to the High Court only on limited grounds, namely a question of law or, in the case of a financial penalty, the amount imposed. Applications for reconsideration and appeals must be made within the prescribed period of 28 days.

Illustrative Example

In *Re Marina Bay Sands Pte Ltd* [2025] SGPDP 6, the PDPC imposed a financial penalty of SGD315,000 on Marina Bay Sands Pte Ltd. This decision illustrates the PDPC's calibrated approach to financial penalties following the 2020 amendments to the PDPA, clarifying that penalties are assessed with reference to factors such as the organisation's annual turnover, the seriousness and duration of the breach, and the extent

of harm or risk posed to individuals, rather than being applied mechanically at the statutory maximum.

Criminal Offences

Section 51 (1) of the PDPA provides for specific criminal offences for persons, including requesting access to, or correction of, another individual's personal data without authority. Under Section 51 (3) of the PDPA, criminal offences for both persons and organisations include:

- evading access/correction requests;
- obstructing enforcement; or
- providing false information to the Commission, an inspector or an authorised officer.

Offenders are liable to fines and/or imprisonment.

Further, Part 9B of the PDPA introduces specific offences targeting egregious mishandling of personal data at the individual level. These provisions make it a criminal offence for an individual to knowingly or recklessly:

- disclose personal data without authorisation;
- use personal data to obtain a wrongful gain or cause harm or loss to another person; or
- re-identify anonymised information without authority.

Individuals convicted of such offences may be subject to fines of up to SGD5,000, imprisonment for up to two years, or both.

1.9 Enforcement Trends

Most enforcement actions taken by the PDPC continue to arise from inadequate data security practices, with breaches of the Protection Obligation forming the largest share of decisions issued in the past 24 months.

On 28 October 2025, the PDPC levied a financial penalty of SGD315,000 against Marina Bay Sands Pte Ltd (MBS) in *Re Marina Bay Sands Pte Ltd* [2025] SGP-DPC 6. This represents the second-largest single fine imposed since the PDPA took effect, and the highest penalty issued following the 2021 PDPA amendments, which raised the maximum financial penalty

from SGD1 million to up to 10% of an organisation's annual turnover in Singapore (subject to a minimum of SGD1 million).

In October 2023, the personal data of approximately 665,000 MBS patrons was unlawfully accessed and exfiltrated, with the compromised information later offered for sale on the dark web. The breach arose from deficiencies during a major software migration in March 2023, where critical security configurations were compiled by a single employee without adequate oversight or verification. The PDPC found that MBS failed to implement reasonable security measures and appropriate post-migration controls, constituting a negligent breach of the protection obligation, particularly given MBS's scale and available resources.

This decision is significant for articulating a structured penalty framework, confirming that, while the enhanced maximum fines introduced in 2021 provide the PDPC with greater headroom, penalties remain proportionate and fact-specific. The PDPC has also emphasised accountability, looking closely at whether organisations had reasonable governance measures, risk assessments and security practices in place prior to an incident.

The decision highlights that organisations must implement robust, layered governance and verification controls, particularly for high-risk activities such as large-scale system migrations, rather than relying solely on individual employees. It also signals the PDPC's increasing focus on deterrence under the enhanced penalty framework, with significant fines possible even where the data involved is not highly sensitive, underscoring the need to prioritise security by design and proactive compliance.

2. Privacy Litigation

2.1 Privacy Litigation Overview

In Singapore, the bulk of data protection enforcement occurs through regulatory measures by the PDPC rather than civil proceedings in the courts.

Under Section 48O(1) of the PDPA, a person who suffers loss or damage directly arising from a contraven-

tion of specified PDPA provisions may bring a private civil action against the organisation in court, without first obtaining a finding from the PDPC. Recent decisions, including the High Court's ruling in *Piper, Martin v Singapore Kindness Movement* [2025] SGHC 173 (*Piper, Martin*) and *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60 (*Reed*), illustrate the approach taken by the courts. Claimants must establish a statutory breach, causation, and actionable loss and damage. Crucially, the Court in *Piper, Martin* emphasised that a "strict causal link" must be established in order for a claim for loss or damage to succeed. Under Section 48O(3), the court may grant injunctive or declaratory relief, award damages, or order any other appropriate remedy.

While the PDPC itself cannot award compensation, non-material harm is compensable in civil proceedings. However, the Singapore courts take a cautious approach towards awarding non-material damages. The Court of Appeal in *Reed* emphasised that courts assess such harm on a fact-specific basis, considering (among other things):

- the sensitivity of the personal data involved;
- the nature and duration of the breach;
- the defendant's conduct (eg, negligent versus malicious);
- the risk of future misuse; and
- the actual impact on the claimant.

2.2 Recent Case Law

Recent case law has clarified key contours of data protection litigation in Singapore, where court actions remain relatively limited. In *Piper, Martin v Singapore Kindness Movement* [2025] SGHC 173, the High Court clarified the parameters of "deemed consent" and the investigation exception under the PDPA, holding that disclosures of personal data must be objectively necessary and reasonable for the stated purpose, even in the context of internal investigations. See **2.1 Privacy Litigation Overview** for the Court's holding on requirements for loss or damages claims to succeed.

Read together with *Reed*, these decisions establish that while non-material harm such as emotional distress can be compensable, mere loss of control over

personal data is insufficient, and liability will turn on necessity, proportionality and proof of actual impact.

2.3 Collective Redress Mechanisms

Singapore does not provide collective redress mechanisms to safeguard the shared interests of multiple individuals.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Singapore currently has no dedicated legislation specifically regulating non-personal data or cross-sector data access comparable to the EU Data Act. The governance of technologies such as IoT, cloud computing and other data processing services falls primarily under the broader PDPA and the Cybersecurity Act 2018, alongside sector-specific guidance from agencies such as the IMDA.

The Data Protection Provisions continue to apply to IoT devices and other connected services that collect personal data, ensuring that organisations deploying such technologies maintain responsible data management practices.

Further, the Amendment Act will introduce a new data portability obligation, which requires an organisation, upon an individual's request, to transfer the individual's personal data in its possession or control (including data generated through IoT and connected devices) to another organisation in a commonly used, machine-readable format. However, it is not yet in force.

Data intermediaries processing data on behalf of others are also subject to specific obligations under the PDPA, namely the protection obligation, the retention limitation obligation, and the data breach notification obligation (where a data intermediary becomes aware, or has reasonable grounds to suspect, that a data breach has occurred involving personal data it processes for another organisation, it is required to inform that organisation promptly).

3.2 Interaction of Data Regulation and Data Protection

See 1.1 Overview of Data and Privacy-Related Laws.

3.3 Rights and Obligations Under Applicable Data Regulation

In Singapore, there is no legislation specifically regulating the use of IoT or other non-personal data services beyond existing frameworks for personal data. Key obligations under the PDPA, set out in 3.1 Objectives and Scope of Data Regulation, continue to apply where personal data is involved, and organisations must implement measures to ensure compliance.

The PDPC issued a Guide to Data Sharing (revised 1 February 2018), which provides guidance on the sharing of personal data:

- within the organisation or group of organisations;
- with a data intermediary; and
- with one or many organisations.

Specifically, compliance with the following are key issues that would arise in the context of data sharing:

- consent obligation;
- purpose limitation obligation;
- notification obligation; and
- transfer limitation obligation.

The IMDA's Internet of Things Cyber Security Guide (published March 2020) for IoT services provides practical obligations for developers, providers and enterprise users, focusing on security principles, risk management and operational best practices, though it explicitly excludes privacy matters. Organisations deploying IoT or cloud-based systems should integrate these baseline security measures with PDPA obligations.

Data intermediaries are also bound by the PDPA and must ensure that they comply with the applicable PDPA obligations set out at 3.1 Objectives and Scope of Data Regulation.

Action items for organisations therefore include, but are not limited to:

- appointing a responsible officer (ie, DPO);
- monitoring data flows; and
- ensuring contractual compliance with data intermediaries.

3.4 Regulators and Enforcement

See 1.7 Regulators.

4. Sectoral Topics

4.1 Use of Cookies

In Singapore, there are no standalone statutory rules that specifically regulate cookies, SDKs or similar tracking technologies. Instead, the PDPA applies where these tools are used to collect, use or disclose personal data. The PDPC has clarified that tracking technologies which process personal data are subject to the same requirements as other forms of personal data processing, while cookies that do not identify individuals generally fall outside the PDPA's scope.

A consent-based framework applies according to the Advisory Guidelines for Selected Topics (revised 23 May 2024). For online functions that a user has expressly requested, organisations may not need to obtain separate consent for the use of cookies where the user understands the purpose and voluntarily provides their data. Where a service cannot operate without cookies that process personal data, consent may be deemed if it is reasonable to expect the individual to provide such data for that activity. This includes activities such as:

- authentication and security;
- user preference;
- network management; and
- streaming content.

However, a user's failure to adjust browser or device settings does not, by itself, amount to consent. In contrast, tracking for purposes such as personalised advertising or profiling generally requires clear and express consent, rather than reliance on implied consent or opt-out models.

4.2 Personalised Advertising and Other Online Marketing Practices

Singapore law does not specifically label or regulate “personalised” or “targeted” advertising as a distinct category. Instead, such practices are governed through the PDPA to the extent they involve the collection, use or disclosure of personal data. Where advertising activities rely on profiling or behavioural analysis that identifies or relates to an individual, organisations are generally required to obtain clear and affirmative opt-in consent.

Where marketing involves sensitive personal data and children’s data, see **1.3 Special Categories of Personal Data** for additional constraints that apply.

4.3 Employment Privacy Law

Under Section 4 (1)(a) and (b) of the PDPA, the Data Protection Provisions do not apply to an employee acting in the course of their employment. However, employers remain subject to the PDPA when collecting, using or disclosing personal data about employees, job applicants and former employees.

Generally, employers are required to notify individuals of the purposes for which their personal data is processed and to obtain consent, unless an exception under the PDPA applies. In practice, employers often rely on deemed consent under Sections 15 and 15A of the PDPA, or on specific statutory exceptions set out in Section 17 and the First and Second Schedules to the PDPA.

Where a job applicant voluntarily provides personal data in the course of a job application, consent is typically deemed for the collection, use and disclosure of that data for purposes reasonably related to evaluating the application. If the applicant is subsequently employed, it would generally be reasonable for the employer to continue using the data for employment-related purposes. Where the employer intends to use the data for purposes outside the scope of deemed consent or any applicable exception, fresh consent must be obtained.

The First and Second Schedules to the PDPA permit the processing of employee personal data without

consent in various employment-related scenarios, including:

- assessing an individual’s suitability, eligibility or qualifications for employment, advancement or continued employment; and
- entering into, managing or terminating their employment relationships, or appointment would not require the consent of their employees.

Note that employers are nevertheless required to notify their employees of purposes of such collection, use or disclosure, by providing the individual with the purpose of processing. Upon request, the employer must provide contact details for a person able to address queries relating to the processing.

In remote working arrangements and bring-your-own-device environments, employers may process personal data to safeguard business systems, manage cybersecurity risks and ensure compliance with internal policies. Such processing may be carried out without consent under the “legitimate interests” exception, subject to the notification obligation and other PDPA requirements.

4.4 Data Protection in M&A

In Singapore, the PDPA permits the collection, use and disclosure of personal data without consent in mergers, acquisitions and asset deals, provided the statutory conditions under Part 4 of the First Schedule to the PDPA are satisfied.

The exception covers transactions where an organisation (X) is a party or a prospective party to a business asset transaction with another organisation (Y), and personal data about an applicable individual of Y:

- is collected from Y by X for the purposes of the business asset transaction;
- is used or disclosed by X in relation to the business asset transaction; or
- is disclosed by Y to X for the purposes of the business transaction.

Where the transaction concerns any part of Y or Y’s business assets, the aforementioned personal data transferred must relate directly to that part.

Due Diligence Stage

Where X is only a prospective party to the transaction, it may collect personal data, and Y may disclose such data, only to the extent necessary to determine whether to proceed with the transaction. In addition, the parties must have entered into an agreement requiring X to use or disclose the personal data solely for purposes connected with the transaction.

Post-Completion Use and Notification

If the transaction proceeds, X may use or disclose the personal data collected only for the same purposes for which Y would have been permitted to do so. Any personal data that does not relate directly to the business or assets acquired must be returned or destroyed. The parties must also notify the affected individuals that the transaction has taken place and that their personal data has been disclosed to X.

Incomplete Transactions

If the transaction does not proceed or is not completed, all personal data collected in connection with the transaction must be returned to Y or securely destroyed.

Change-of-Control and Indirect Transactions

Similar rules apply where the transaction involves the transfer of an interest in a third organisation, such as a share sale.

5. International Considerations

5.1 Restrictions on International Data Transfers

In Singapore, the PDPA regulates cross-border personal data transfers. Non-personal data is generally not subject to transfer restrictions unless sector-specific or cybersecurity laws apply. While a “transfer” is not expressly defined in the PDPA, it would broadly cover any disclosure, sending or making available of personal data to a recipient outside Singapore, whether directly or through remote access.

Pursuant to Section 26 of the PDPA, organisations may only transfer personal data overseas if they have taken reasonable steps to ensure that the recipient is subject to binding obligations that afford a level of

protection comparable to the PDPA. Under the PDP Regulations, such obligations may arise from:

- any law;
- any contract requiring the overseas recipient to afford the transferred personal data a level of protection comparable to that under the PDPA, and which identifies the countries and territories to which the personal data may be transferred under the contract;
- any binding corporate rules (in cases where a recipient is an organisation related to the transferring organisation) that require every recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specify:
 - (a) the recipients of the transferred personal data to which the binding corporate rules apply;
 - (b) the countries and territories to which the personal data may be transferred under the binding corporate rules; and
 - (c) the rights and obligations provided by the binding corporate rules; or
- any other legally binding instrument.

In relation to binding corporate rules, the PDP Regulations define a recipient as being related to the transferring organisation if:

- the recipient, directly or indirectly, controls the transferring organisation;
- the recipient is, directly or indirectly, controlled by the transferring organisation; or
- the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

The PDP Regulations expressly recognise certification under the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) frameworks as an accepted basis for international data transfers. Where an overseas recipient holds a relevant CBPR or PRP certification that is recognised in its jurisdiction, it is deemed to be subject to enforceable obligations ensuring that the transferred personal data is protected to a standard comparable to that required under the PDPA.

5.2 Government Notifications and Approvals

Singapore does not impose any registration, filing, notification or prior approval requirements with regulatory authorities solely for the purpose of transferring data overseas.

5.3 Data Localisation Requirements

Singapore does not impose explicit data localisation or data residency requirements under the PDPA. Organisations are therefore not obliged to retain personal data, or copies of such data, physically within Singapore, even where the data is stored or processed abroad.

Remote access to personal data from outside Singapore is treated in practice as a form of cross-border transfer. It is permitted so long as the organisation complies with the PDPA's transfer limitation obligation, including taking steps to ensure that overseas recipients or access arrangements afford a level of protection comparable to that required under Singapore law.

5.4 Blocking Statutes

Singapore does not maintain a general "blocking statute" or foreign-judgment control regime that restricts compliance with foreign discovery orders or sanctions. Nevertheless, cross-border disclosures of data are constrained by existing confidentiality and data protection laws. In particular, Section 26 of the PDPA limits the transfer of personal data outside Singapore unless the transferring organisation ensures that the recipient is subject to legally enforceable safeguards providing a level of protection comparable to the PDPA.

Separately, disclosures may be prohibited under the Official Secrets Act and the Statutory Bodies and Government Companies (Protection of Secrecy) Act 1983, which prevents the disclosure of official government-related documents and information.

5.5 Recent Developments

In June 2025, the Global Cross-Border Privacy Rules (CBPR) Forum formally launched the Global CBPR and Privacy Recognition for Processors certification systems, marking a significant development in the facilitation of international personal data transfers.

- The Global CBPR framework establishes a single certification that organisations can rely on to transfer personal data across all participating economies, which currently include Singapore, the United States, Japan, Australia, Canada and several other jurisdictions. Certification is obtained through accredited Accountability Agents, with the IMDA acting as the designated authority in Singapore.
- In Singapore, Global CBPR certification is recognised under the PDPA as a lawful mechanism for overseas data transfers, reducing the need for organisations to implement additional contractual or organisational safeguards when transferring personal data to other member economies.
- Looking ahead, the Global CBPR Forum has signalled plans to expand membership beyond the current group of economies, continuing to build its network of certified organisations – developments that are expected to further shape Singapore's approach to cross-border data transfer compliance.

Trends and Developments

Contributed by:

Chong Kin Lim, David N. Alfred and Anastasia Chen
Drew & Napier LLC

Drew & Napier LLC established a dedicated Data Protection, Privacy and Cybersecurity Practice to leverage its unrivalled experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. The firm represents many regional companies, multinationals, industry associations, government bodies and regulators, and regularly assists them on a wide range of matters in Singapore and ASEAN member countries.

At the forefront of data protection law in Singapore since 2013, the Data Protection, Privacy & Cybersecurity Practice Group has worked on significant data protection enforcement cases and appeals, including those involving cybersecurity elements. Building on its experience in this field, the Drew Data Protection & Cybersecurity Academy was established in 2020 to offer clients services relating to data protection and cybersecurity compliance, including training, consulting and external data protection officer services.

Authors



Chong Kin Lim heads Drew & Napier's highly regarded TMT practice group. His clients include telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.

Chong Kin has worked on every significant development in the Singapore TMT market, and continues to play a key role in the development of sectoral competition regulation in Singapore. He was the lead external counsel in the liberalisation of the telecommunications, media and postal sectors, and has assisted regulators in conceptualising and drafting "first-of-its-kind" sectoral competition legislation and frameworks.



David N. Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy & Cybersecurity Practice Group. He is concurrently co-head and programme director of the Drew Data Protection &

Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 25 years' experience advising on a broad range of matters relating to digital technology,

telecommunications and the internet. He has substantial experience advising on data protection and cybersecurity compliance, regulatory enforcement, data breaches and international aspects of data protection. Prior to joining the firm, David was the first Chief Counsel of Singapore's data protection authority, the Personal Data Protection Commission.



Anastasia Chen is a director of Drew & Napier LLC and deputy head of the firm's Data Protection, Privacy & Cybersecurity Practice Group. Prior to joining the firm, Anastasia was Deputy Chief Counsel to Singapore's

Personal Data Protection Commission (PDPC) and Info-communications Media Development Authority (IMDA) for over nine years, during which she served as lead counsel for PDPC's matters, IMDA's procurement and intellectual property portfolios, as well as IMDA's Data Administration Group. She has received accolades from legal publications, with clients commending her deep industry and regulatory expertise, as well as legal acumen, especially when dealing with novel problems.

Drew & Napier LLC

10 Collyer Quay
10th Floor
Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Fax: +65 6535 4864
Email: mail@drewnapier.com
Web: www.drewnapier.com



Introduction

Businesses in Singapore are increasingly confronted with the challenge of staying compliant and secure with data protection regulations, in the face of rapid adoption of digital services, increased data sharing, and AI risks. That said, the Personal Data Protection Commission (PDPC) remains cognisant and responsive, refining, administering and enforcing Singapore's Personal Data Protection Act (PDPA) in ways that support and balance accountability and innovation.

This chapter of the guide unpacks the following topics which have recently taken on increasing relevance:

- cross-border data transfers;
- protection of data in the context of AI deployment;
- phasing out of National Registration Identity Card (NRIC) numbers for authentication;
- amendments to the Public Sector (Governance) Act (PSGA); and
- local enforcement trends.

Cross-Border Data Transfers

Cross-border data transfers remain central to Singapore's digital economy, supporting e-commerce and other digitally enabled functions such as data analytics and AI deployment. As organisations increasingly rely on global technology vendors and distributed data infrastructures, compliance with cross-border transfer rules continues to be both an operational necessity and a strategic consideration.

Cross-border data transfers are governed by Section 26 of the PDPA, which provides that organisations must ensure that any overseas recipient provides a

standard of protection to the transferred personal data that is at least comparable to the PDPA. In practice, this is typically achieved through contractual safeguards.

EU-Singapore Digital Trade Agreement (EUSDTA)

A recent development in this area is the entry into force of the EUSDTA on 1 February 2026. As a key digital trade partner of the European Union, Singapore's entry into the EUSDTA reflects both parties' commitment to open, rules-based digital trade, while upholding strong protections for personal data and privacy in cross-border digital transactions.

The EUSDTA introduces binding commitments designed to facilitate cross-border digital transactions and reduce regulatory uncertainty. These include provisions to:

- strengthen online consumer protection;
- protect personal data and privacy;
- promote paperless trade;
- recognise electronic signatures and contracts; and
- prohibit unjustified data localisation requirements or forced transfers of source code.

The EUSDTA is particularly relevant for businesses operating between Singapore and the EU that rely on cloud-based platforms, cross-border analytics or regional technology providers. While the EUSDTA does not replace domestic data protection obligations, it signals a continued policy direction towards enabling trusted data flows through interoperable digital trade rules.

Contractual and certification mechanisms

The PDPC continues to recognise a range of practical mechanisms to facilitate cross-border transfers that are compliant with the PDPA's transfer limitation obligation.

At a regional level, the ASEAN Model Contractual Clauses are recognised and encouraged by the PDPC as a practical contractual mechanism, particularly for organisations with intra-group or vendor-related transfers within South-East Asia. These standardised clauses are designed to align with the ASEAN Framework on Personal Data Protection 2016 and can help streamline negotiations across multiple ASEAN jurisdictions.

In addition, Regulation 12 of the Personal Data Protection Regulations 2021 recognises certifications under the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems as mechanisms that satisfy the transfer limitation obligation. These certifications provide a structured, internationally recognised approach to demonstrating comparable data protection standards across participating economies.

Building on the aforementioned cross-border privacy mechanisms, the Global CBPR and Global PRP systems were introduced in June 2025 as broader international certification frameworks. While Singapore's regulations currently recognise only the APEC CBPR and PRP certifications, the Global CBPR framework reflects a wider trend towards interoperable, certification-based transfer regimes.

Taken together, these developments point to an increasingly layered cross-border data governance environment. Businesses operating across multiple jurisdictions should therefore consider both treaty-level developments, such as the EU-Singapore DTA, and practical compliance tools, such as contractual clauses and recognised certifications, when structuring their data transfer arrangements.

Data Protection in the Context of AI Deployment

Singapore introduced three new initiatives in July 2025:

- the new Global AI Assurance Sandbox;
- a new privacy enhancing technology (PET) adoption guide; and
- the Singapore Standard for Data Protection.

The Global AI Assurance Sandbox

The Global AI Assurance Sandbox aims to provide a conducive environment for organisations to trial responsible AI applications, offering tools, resources and a controlled setting for practical testing. Building on insights from an earlier pilot phase, the sandbox now covers additional AI archetypes, such as agentic AI, as well as emerging risks including data leakage and prompt injection vulnerabilities. It addresses a broad range of AI-related risks and is also relevant from a data protection perspective, as it enables organisations to assess how their AI systems manage data-related risks before full-scale deployment. The sandbox may also be opened to sectoral regulators to test governance or assurance approaches, with insights feeding into future policy guidance and potential accreditation frameworks for AI testers.

PETs Adoption Guide

PETs protect personal data while allowing organisations to use such data for AI development and training and are increasingly positioned as practical tools to enable data-driven innovation without compromising privacy. First introduced in 2022 by the IMDA and PDPC, Singapore's PET Sandbox now explores how PETs can be applied to generative AI use cases while managing associated data protection risks. Drawing on insights from these sandbox projects, IMDA has released a new PETs Adoption Guide to help organisations deploy PETs and derive greater value from their data. The guide includes a "PETs Use Case Evaluation Tool" to assist organisations in identifying suitable PET solutions, as well as an "Implementation Checklist" to support the end-to-end adoption process. IMDA has emphasised that the guide is intended to be a "living document", with ongoing refinements based on industry feedback and additional use cases.

The Singapore Standard for Data Protection

The Data Protection Trustmark was elevated into a new Singapore Standard (SS 714:2025), aligning it with international data protection benchmarks and best practices. Organisations can now apply for certi-

fication under this enhanced framework, which serves as a recognised mark of accountable data protection practices and provides assurance to consumers and regulators on the organisation's handling of personal data. The new standard introduces clearer requirements in areas such as third-party management and overseas data transfers and is overseen by the Singapore Accreditation Council to ensure certification assessments meet globally recognised standards. For organisations, certification under the Singapore Standard serves as an externally recognised indicator of robust and accountable data governance.

For businesses deploying AI systems, the developments signal increasing regulatory expectations around testing, assurance and accountable data practices. Organisations should consider whether PETs can be incorporated into AI development pipelines, assess participation in regulatory sandboxes where appropriate, and evaluate certification frameworks such as the Data Protection Trustmark as part of their broader AI and data governance strategies.

Phasing Out of NRIC Numbers for Authentication

In February 2026, the PDPC announced that private organisations must cease using NRIC numbers for authentication purposes by 31 December 2026. Organisations that continue to rely on full or partial NRIC numbers as authentication credentials may be found to have breached Section 24 of the PDPA for failing to implement reasonable security arrangements, with enforcement expected to intensify from 1 January 2027.

This development builds on the June 2025 joint advisory issued by the PDPC and the Cyber Security Agency of Singapore, which clarified that NRIC numbers should not be used as authentication credentials. Practices such as using NRIC numbers as default passwords, or combining them with easily obtainable information like names or dates of birth, have been identified as insecure because NRIC numbers are widely used identifiers and may be readily exposed or guessed.

For businesses, the announcement may require significant changes to existing systems and processes. Many organisations, particularly in sectors such as tel-

ecommunications, healthcare and financial services, have historically relied on NRIC-based verification for user portals and access to digital documents. These organisations will need to review their existing authentication workflows and implement more secure alternatives, such as one-time passwords, authenticator applications or multi-factor authentication.

More broadly, the phase-out reflects the PDPC's continued emphasis on security-by-design and the expectation that authentication methods should be proportionate to the sensitivity of the personal data involved. Organisations with legacy systems or large customer bases should therefore prioritise transition planning well ahead of the 31 December 2026 deadline.

Amendments to the PSGA

In January 2026, Parliament passed amendments to the PSGA, marking a notable development in Singapore's public-sector data governance framework. The amendments are intended to streamline data-sharing processes to support the more efficient delivery of public services, including by extending the data-sharing regime to trusted external partners beyond the public sector engaged by the government.

The amendments permit public agencies to share data with such trusted external partners, provided that the sharing serves the same seven public-interest purposes recognised under the Act. This represents a measured expansion of the original framework, which previously focused on data sharing among public agencies. The change reflects the practical reality that many public services are delivered in collaboration with external organisations, such as social service providers, research institutions, and private-sector vendors, which may require access to government-held data to perform their functions effectively.

To address the risks associated with extending data access beyond the public sector, the amendments introduce three key safeguards for data sharing with external partners:

- data may only be shared where it serves one of the legitimate public-interest purposes specified under the PSGA;

- the sharing arrangement must be authorised by the relevant Minister or a delegated authority, with the approval specifying the purpose of the sharing, the scope of data involved, and the external partners permitted to receive it; and
- external partners must be subject to contractually binding terms of use that impose data protection and security requirements at least equivalent to those applicable to public agencies.

Individuals working for such partners may also face criminal liability for misuse of shared data, with penalties aligned to those applicable to public officers under the PSGA.

The amendments also clarify that public agencies may use, and not merely share, data for the purposes specified under the PSGA, while remaining subject to existing internal governance and security requirements. Importantly, the PSGA does not override confidentiality obligations imposed under other written laws, legal privilege or contractual arrangements.

For the private sector, the amendments are particularly relevant to organisations that provide services to, or partner with, government agencies. External partners, such as technology vendors, data analytics providers and contractors, may now receive government-held data under a statutory framework, leading to more structured arrangements with public-sector-aligned data protection, security and accountability requirements. Furthermore, these external partners should expect heightened scrutiny of their data governance practices and be prepared to meet public-sector standards of accountability and security.

Enforcement Trends

The PDPC has been taking a strong enforcement stance against breaches of the various obligations under the PDPA. In *Re Marina Bay Sands Pte Ltd* [2025] SGPDP 6, the PDPC meted out its second largest financial penalty (to date) of SGD315,000, having factored in the annual turnover of the organisation in determining the financial penalty amount.

Clarity on financial penalty framework

From 1 October 2022, Parliament raised the maximum financial penalty for large organisations with annual

turnovers in Singapore over SGD10 million, to 10% of their annual turnovers.

The PDPC has now, for the first time, in *Re Marina Bay Sands Pte Ltd* [2025] SGPDP 6, articulated key aspects of its financial penalty framework for determining the quantum of financial penalties under the PDPA.

In brief, Marina Bay Sands (MBS) is an integrated resort operator that runs, among other things, two membership programmes: Sands Rewards Lifestyle and ArtScience Friend. In October 2023, the personal data of 665,495 MBS patrons was illegally accessed and exfiltrated by unknown actors. The affected data, including names and contact details that identified MBS's patrons, was later found for sale on the dark web. MBS admitted to breaching the protection obligation, by failing to take reasonable security measures to protect the personal data in its possession.

The PDPC's financial penalty framework is subject to the following guiding principles.

- The framework aims to effectively deter non-compliance with the PDPA, while ensuring proportionality to the seriousness of the non-compliance.
- When considering the relative weight to be given to effective deterrence and proportionality, consideration has to be given to the PDPA's overarching balance of the right of individuals to protect their personal data and organisations' need to process personal data for legitimate purposes.
- There should be like and consistent treatment in the two-tiered financial penalty regime for organisations with annual turnovers of SGD10 million and below, and organisations with annual turnovers above SGD10 million. Annual turnover size should be accorded more weight for organisations with annual turnovers above SGD10 million. Other relevant factors must be given similar weight in like cases.
- The financial penalty framework must be applied in a fact-sensitive manner.

With these in mind, the Penalty Framework comprises the following steps.

- *Preliminary step* – The PDPC first identifies the applicable statutory maximum financial penalty under Section 48J(3) of the PDPA. It then determines an appropriate percentage rate or quantum cap, not exceeding that statutory maximum, based on the nature of the contravention. In general, intentional breaches attract higher rates than negligent ones, and this exercise establishes the maximum financial penalty applicable for the case before the subsequent steps of the framework are applied.

- A *five-step methodology* then applies.

- (a) Step 1 – Identification of level of culpability and harm. The PDPC assesses all relevant factors, including the nature, gravity and duration of the non-compliance, to determine the organisation's level of culpability as "low", "medium" or "high". It will also assess whether the level of harm is "slight", "moderate" or "severe", taking into account factors such as the type and sensitivity of the affected data, the number of individuals impacted, and the extent of actual or potential harm.

- (b) Step 2 – Calculation of the starting financial penalty. Based on the assessed levels of culpability and harm in Step 1, the PDPC identifies the corresponding starting range and determines an appropriate starting financial penalty within that range.

- (c) Step 3 – Adjustment for aggravating and mitigating factors. The PDPC then adjusts the starting financial penalty identified in Step 2 to reflect relevant aggravating and mitigating considerations, such as the organisation's co-operation, remedial actions, prior compliance record or any benefit derived from the contravention.

- (d) Step 4 – The PDPC considers whether the proposed financial penalty would adversely affect the organisation's ability to continue its usual operations, based on the available evidence. Where appropriate, it may extend the payment timeline, allow instalment payments or reduce the penalty amount.

- (e) Step 5 – Final adjustments. The PDPC conducts a final review of the quantum to ensure that the resulting financial penalty is both effective as a deterrent and proportionate in the circumstances of the case.

Applying this framework, the PDPC found that the maximum financial penalty applicable to MBS was 10% of its turnover. Applying Step 1, MBS's level of culpability was low, but there was a moderate level of harm due to the large number of affected individuals. The PDPC then determined the starting financial penalty within the low-moderate band and adjusted this to account for relevant mitigating factors, including MBS's voluntary notification to affected individuals and prompt remedial measures. This ultimately resulted in a reduced financial penalty of SGD315,000, which the PDPC found would not adversely affect MBS's ability to carry out its usual operations.

The decision signals the PDPC's increasing emphasis on deterrence, as substantial penalties may be imposed even where the compromised data is not highly sensitive. It also underscores the regulator's expectations that organisations implement robust operational controls, rather than relying solely on individual employees, particularly where large volumes of personal data are involved. Businesses should place increased emphasis on data protection and cybersecurity.

Conclusion

Singapore's data protection landscape is evolving alongside developments in digital trade, AI and data-driven public services, with a clear emphasis on enabling innovation while strengthening accountability and security obligations.

For businesses, compliance should not be treated as a static or one-off exercise. Recent developments across digital services, AI governance, authentication practices and public-sector data sharing, coupled with increased enforcement scrutiny, point to a more integrated, risk-based data environment.

SOUTH KOREA

Law and Practice

Contributed by:

Brian Tae-Hyun Chung, Haewon Han, Jung-Chull Lee and Ari Yoon
Kim & Chang



Contents

- 1. Legal and Regulatory Framework p.434**
 - 1.1 Overview of Data and Privacy-Related Laws p.434
 - 1.2 Rights and Obligations p.434
 - 1.3 Special Categories of Personal Data p.435
 - 1.4 Processing of Personal Data for Research and Development Purposes p.436
 - 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.436
 - 1.6 Data Breach Requirement p.437
 - 1.7 Regulators p.438
 - 1.8 Enforcement Proceedings and Fines p.438
 - 1.9 Enforcement Trends p.439
- 2. Privacy Litigation p.439**
 - 2.1 Privacy Litigation Overview p.439
 - 2.2 Recent Case Law p.439
 - 2.3 Collective Redress Mechanisms p.440
- 3. Requirements for the Protection and Processing of Non-Personal Data p.441**
 - 3.1 Objectives and Scope of Data Regulation p.441
 - 3.2 Interaction of Data Regulation and Data Protection p.441
 - 3.3 Rights and Obligations Under Applicable Data Regulation p.441
 - 3.4 Regulators and Enforcement p.442
- 4. Sectoral Topics p.442**
 - 4.1 Use of Cookies p.442
 - 4.2 Personalised Advertising and Other Online Marketing Practices p.442
 - 4.3 Employment Privacy Law p.443
 - 4.4 Data Protection in M&A p.443
- 5. International Considerations p.444**
 - 5.1 Restrictions on International Data Transfers p.444
 - 5.2 Government Notifications and Approvals p.445
 - 5.3 Data Localisation Requirements p.445
 - 5.4 Blocking Statutes p.445
 - 5.5 Recent Developments p.445

Kim & Chang has a privacy and data security practice that assists clients with better understanding the extensive Korean privacy and data security law requirements, and providing company-wide compliance audits and risk assessments of their current personal information-processing practices. It offers expertise in sectors and areas including e-commerce, insurance, banking, healthcare, TMT, HR, compliance, criminal defence and litigation, providing a holistic service that is suited to its clients' needs. The pri-

vacy and data security practice within the firm has expertise in laws such as the Personal Information Protection Act and others that have a bearing on information security and data protection. The practice provides comprehensive advice that allows clients to effectively mitigate and manage the risk of civil, criminal and administrative liability, and is able to advise not only on legal compliance but also on technical compliance – it is recognised as one of the leaders in this field in Korea.

Authors



Brian Tae-Hyun Chung is a foreign attorney at Kim & Chang. He practises primarily in antitrust and competition, privacy and game, resorts and entertainment. As a member of the firm's privacy and data

security practice, Mr Chung provides clients with expert assistance in privacy and data protection matters, specialising in compliance with Korean privacy laws and administrative, criminal and civil proceedings arising out of data breach cases.



Haewon Han is an attorney at Kim & Chang. She practises primarily in the field of privacy and TMT. She has successfully defended businesses in various investigation by the Personal Information Protection Commission (a

regulatory body for data privacy projects) and has also helped a number of businesses in data privacy compliance projects.



Jung-Chull Lee is a foreign attorney at Kim & Chang. His practice covers a broad range of legal matters, including TMT and privacy. As a member of the firm's privacy and data security practice, he has extensive

experience in advising multinational corporations on privacy and data protection as well as investigations conducted by government authorities, including the Personal Information Protection Commission.



Ari Yoon is an attorney at Kim & Chang. She practises primarily in the field of privacy, especially in the healthcare and IT industries. As a leading expert in the area of data regulation and privacy, Ms Yoon

engages in close dialogue with her clients, advising on day-to-day data privacy issues, and has successfully led various data privacy projects aimed at establishing and improving a company's overall data privacy compliance. She is a member of the Personal Information Dispute Mediation Committee, and has served as a director of the Korea Data Law and Policy Society and AI Law Society.

Kim & Chang

39, Sajik-ro 8-gil
Jongno-gu
Seoul 03170
Korea

Tel: +82 2 3703 1114
Fax: +82 2 737 9091/9092
Email: lawkim@kimchang.com
Web: www.kimchang.com

KIM & CHANG

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Personal Information Protection Act (PIPA) is the overarching privacy legislation in Korea. Other statutes governing particular types of personal information include the Credit Information Use and Protection Act (the “Credit Information Act”) and the Act on the Protection and Use of Location Information (the “Location Information Act”). The Act on Promotion of Information and Communications Network Utilisation and Information Protection, etc (the “Network Act”) also deals with some privacy issues, such as sending advertising information, appointing a Chief Information Security Officer and issuing certification for information security management systems.

While Korean constitutional law does not expressly guarantee rights related to personal information, the Constitutional Court’s position is that the right to self-determination of personal information derives from general personality rights, and the right to privacy and freedom and is thus protected under the Constitution.

The National Assembly passed the proposed bill for the Framework Act on the Development of Artificial Intelligence and the Establishment of a Foundation for Reliability (the “AI Framework Act”), which was set to take effect on 22 January 2026. This statute is Korea’s first foundational law in the field of AI, aiming to ensure transparency and safety by imposing various obligations on AI service providers.

Regarding extraterritorial reach, both the Network Act and the AI Framework Act expressly provide for extraterritorial application, and they apply to acts conducted outside Korea if such acts affect the Korean market or users (see Article 5-1 of the Network Act and Article 4 of the AI Framework Act).

By contrast, the PIPA does not contain an explicit provision on extraterritorial application. Nevertheless, the Personal Information Protection Commission (PIPC) explains in its Guideline on the Application of the PIPA to Overseas Business Operators (published in April 2024) that the applicability of the PIPA should be assessed by reference to factors such as:

- whether goods or services are offered to Korean data subject;
- whether the relevant activities have an impact on Korea or on Korean data subjects; and
- whether the business has an establishment within Korean territory.

1.2 Rights and Obligations

The PIPA establishes the following general principles governing the processing of personal data.

- Purpose specification and data minimisation: the purpose of processing must be clearly specified and personal data may be collected lawfully only to the extent necessary to achieve that purpose.
- Purpose limitation: personal data must be processed within the scope of the stated purpose of collection. Any use beyond that purpose is prohibited.
- Data accuracy: data controllers must ensure that personal data is accurate, complete and kept up to date, and must maintain appropriate controls to that end.
- Security safeguards: data controllers must implement appropriate technical and administrative measures by taking into account the level of risk associated to ensure the secure processing and management of personal data.
- Transparency and protection of data subject rights: data controllers must make their privacy policies publicly available and ensure the effective exercise of data subject rights, including the right of access.
- Minimisation of privacy intrusion: processing activities should be designed to minimise infringement of data subjects’ privacy.
- Anonymisation or pseudonymisation: where anonymisation is feasible, anonymised data should preferably be used; if not, personal data should be pseudonymised.
- Accountability and trust: data controllers should build trust with data subjects through compliance with and faithful implementation of their statutory obligations.

The legal basis on which a data controller may rely varies depending on the type of personal data processing. For the collection and use of personal data, permissible legal bases include (among others):

- the data subject's consent;
- where processing is expressly authorised by applicable law (ie, statutory authorisation);
- where processing is necessary for the performance of a contract to which the data subject is a party (ie, contractual necessity); and
- where processing is necessary to pursue the legitimate interests of the data controller, subject to applicable statutory limitations (ie, legitimate interests basis).

The legal bases applicable to third-party provision of personal information, delegation of processing to a third party, and overseas transfers of personal data are subject to additional requirements and are addressed separately. Please refer to **5.1 Restrictions on International Data Transfers**.

Regarding data subjects' rights, under the PIPA, data subjects have a broad set of rights, including:

- the right to request access to their personal data;
- the right of data portability;
- the right to request rectification, deletion and suspension of processing; and
- the right to withdraw consent.

They also have the right to object to the automated decision-making and to request an explanation of how such processing is carried out.

Under the Credit Information Act, credit data subjects have:

- the right to request data portability;
- the right to be notified of the credit information based on which a transaction refusal was based;
- the right to request explanations of, and raise objections to, the results of automated assessments;
- the right to withdraw consent to the transfer of personal credit information; and
- the right to request cessation of contact.

Credit data subjects may also request notification of credit inquiry records, free access to their credit information, and disclosure or access to information con-

cerning changes in creditors related to their personal credit information.

Under the Location Information Act, personal location information subjects have:

- the right to withdraw consent;
- the right to request suspension of processing; and
- the right to request access to, notification of, and correction of their personal location information.

For compliance, the data controller must establish and rely on an appropriate legal basis corresponding to each type of personal data-processing activity. In addition, the PIPA requires data controllers to implement technical, administrative and physical security measures necessary to ensure the security of personal data in accordance with the *Standards for Measures to Ensure the Security of Personal Information*, a notice published by the PIPC. Data controllers are also required to establish and publicly disclose a privacy policy that accurately describes their personal processing practices to ensure transparency.

1.3 Special Categories of Personal Data

Under the PIPA, special categories of personal data are:

- sensitive information; and
- unique identification information.

Sensitive information is personal information relating to an individual's ideology or beliefs, membership in or withdrawal from a labour union or a political party, political opinions, health or sex life, genetic information, criminal history, biometric data used for identification purposes, and race or ethnicity, where the processing of such information may seriously infringe upon one's privacy.

Unique identification information includes resident registration numbers, passport numbers, driver's licence numbers, and foreigner registration numbers.

Because both sensitive information and unique identification information are subject to heightened protection (ie, requiring separate legal bases and enhanced

security measures compared to general personal data), particular caution is required in their processing.

Additionally, the PIPA requires the consent of a legal guardian for the processing of personal information of children under the age of 14, and allows the legal guardian to exercise the data subject's rights on behalf of the child.

Similarly, the Location Information Act also requires legal guardian consent for the processing of personal location information of children under the age of 14. The regulator has taken the position that, for children aged 8 to under 14, the lawful processing of personal location information requires both the legal guardian's consent and the child's own consent (however, this issue remains subject to ongoing litigation). Under the Location Information Act, the legal guardian may likewise exercise the rights of a personal location information subject on the child's behalf.

1.4 Processing of Personal Data for Research and Development Purposes

The PIPA permits the processing of pseudonymised information without the data subject's consent if such processing is necessary for statistical purposes, scientific research, or the preservation of records for the public interest.

If pseudonymised information is provided to a third party, it must not include any information that would enable the identification of an individual, and all other regulatory requirements applicable to the processing of pseudonymised information must be complied with.

Additionally, in the case of healthcare providers, the processing of medical information may be subject to further restrictions under the Medical Service Act and other applicable sector-specific laws and regulations.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

The AI Framework Act

The AI Framework Act was passed by the National Assembly on 26 December 2024 and came into effect on 22 January 2026. This legislation establishes obligations for providers of high-impact, generative and high-performance AI services to ensure safety and

transparency. It does not designate any categories of AI as prohibited. Key provisions include the following.

Extraterritorial regulation and domestic agent system

The AI Framework Act can apply to actions taken outside Korea if they affect the Korean market or users. AI service providers without a business presence in Korea must designate a domestic agent and report to the Minister of Science and ICT (MSIT) if they meet certain criteria.

Obligations for high-impact AI

AI business operators providing high-impact AI products or services using such technology are required to pre-assess their AI technology to determine whether it is high-impact, give advance notice to users, implement comprehensive safety and reliability measures to ensure no undue risk, and possibly conduct an impact assessment on individuals' fundamental rights and provide explanations to individuals affected by high-impact AI of the logic and principles behind AI-generated outcomes.

The high-impact AI category includes AI systems used in areas involving decisions that may have a material effect on individual's rights or obligations, such as energy, drinking water, healthcare, nuclear power, and decision-making related to employment or credit assessment for loans.

Obligations for generative AI

AI business operators that offer products or services using generative AI technology are required to give advance notice to users that the products or services are powered by generative AI, label products or services as being created by generative AI, and clearly label deepfake content.

Obligations for high-performance AI

AI business operators offering AI with a significant cumulative amount of compute used for training that surpasses a certain threshold are required to identify, assess and mitigate risks throughout the AI life cycle, as well as establish a risk-management system to monitor and address AI-related safety issues and report the results to the MSIT.

Further Details

Details such as the scope of AI-related obligations will be determined by the subordinate laws and regulations. As the subordinate laws and guidelines for the AI Framework Act have not yet been finalised as of the date of this article, it is necessary to continue monitoring legislative developments.

The AI Framework Act relies on the existing PIPA regulations when it comes to personal information. The PIPC plays a key role in shaping these regulations.

- The PIPC is actively developing AI-related policies, having published various guidelines that define the application principles and standards of the PIPA. These guidelines cover topics including generative AI, privacy risk management model for safe use of AI, publicly disclosed information, unstructured data, biometric information, synthetic data, mobile image devices and transparency.
- In 2023, the PIPA was amended to introduce regulations on automated decisions made by fully automated systems, such as AI. Under these regulations, data subjects have the right to request explanations of automated decisions and, in some cases, the right to refuse them. Data controllers must disclose the standards and procedures for these decisions and how personal information is processed, ensuring that data subjects can easily understand this information.

The PIPC believes that applying the principle of personal information protection in a balanced manner is essential for maximising the benefits and opportunities of using AI, while minimising the risk of personal information infringement potentially caused by AI. In particular, the PIPC seeks to promote the use of data by resolving legal uncertainties through the following systems:

- regulatory sandbox – under certain conditions, products or services using new AI technologies can first be released, tested and verified without being subject to all or part of the existing personal information regulations, thereby promoting the use of data necessary for the development and provision of AI; and

- preliminary adequacy review system – if it is uncertain whether a service provider can comply with the PIPA in the course of planning new technologies or services such as AI, the service provider and the PIPC can work together to come up with a plan to resolve legal uncertainties.

1.6 Data Breach Requirement

A data controller is required to:

- report a data breach to the PIPC or the Korea Internet & Security Agency (KISA); and
- notify the affected data subjects within 72 hours from the time it becomes aware of the breach.

While the reporting obligation to the authorities is triggered only when certain statutory thresholds are met, notification to data subjects is mandatory in all cases where a data breach has occurred.

Separately, even where no data breach has occurred, online service providers may be subject to additional reporting obligations under other applicable laws. For example, if a cybersecurity incident affecting information networks or related systems is identified, a report must generally be filed within 24 hours. Depending on the interplay between applicable laws, certain reporting or notification obligations may be exempted. Accordingly, in practice, business operators must carefully review the laws applicable to each incident and determine whether they bear reporting or notification obligations.

In the event of a data breach or a cybersecurity incident, investigations are typically conducted by the PIPC and the MSIT, with the assistance of the KISA. If necessary, the MSIT may also form a public-private joint investigation task force for the investigation. In addition, the National Assembly may conduct audits or hold hearings, and the National Policy Agency may carry out witness investigations. Such investigations by different authorities often proceed simultaneously.

When a data breach takes place, data subjects may file an application for collective dispute mediation under the PIPA. Although the PIPA does not provide for a class action mechanism for damages, data subjects may individually bring civil claims for damages before

the courts. If a data controller refuses to participate in collective dispute mediation or declines to accept the mediation outcome, consumer organisations or civic groups designated under the PIPA may file an injunctive action with the court seeking to prohibit or suspend the infringing conduct.

1.7 Regulators

The key regulators are as follows:

- the PIPC (in charge of enforcing the PIPA);
- the Korea Media and Communications Commission (KMCC) (in charge of enforcing the Network Act and the Location Information Act);
- the KISA (conducts tasks related to information security as delegated by the PIPC, the KMCC and MSIT);
- the Financial Services Commission (FSC) (in charge of enforcing the Credit Information Act); and
- the MSIT (in charge of enforcing the AI Framework Act).

The PIPC, the KMCC, the FSC and the MSIT have the authority to conduct investigations – for example, through requests for information and on-site inspections. While the KISA does not have law enforcement authority by itself, it often conducts investigations on behalf of the PIPC, the KMCC and the MSIT.

Although investigations are often initiated when data controllers report a data breach or personal information infringement to the regulators, the regulators also conduct regular as well as ad hoc inspections based on the relevant laws and regulations. The regulators – including the PIPC, KMCC and FSC – issue an annual work plan at the beginning of each year, and this helps businesses to anticipate which industry sectors may be a target each year. Investigations can also be triggered when there is media coverage of a specific incident or issue. In data breaches where multiple regulators are involved, investigations are often conducted in parallel. While the guidance issued by each regulator is not legally binding, it effectively serves as the practical standard for enforcement in practice.

The PIPC has recently declared its intention to “secure leadership in global personal information regulatory norms”. To that end, it expressed its commitment to

strengthening international co-operation, providing more detailed guidance for foreign business operators, and analysing major enforcement actions taken by overseas regulators. Through these efforts, the PIPC aims to enhance its global investigative capabilities and establish an international information-sharing network.

1.8 Enforcement Proceedings and Fines

Regulators must provide a written notice before commencing an investigation, as well as prior to imposing an administrative disposition. In order for an administrative disposition to be lawful, not only should the procedures be lawful but the content of such disposition must also satisfy the principle of proportionality.

Where a data controller intends to object to an administrative fine, it may do so in writing and go through a trial. For other administrative dispositions, it may file an administrative appeal or an administrative lawsuit.

The administrative fine and the administrative penalty are both monetary sanctions for administrative violations, but they differ in the nature and severity of the offences they address. Typically, administrative fines are imposed for minor violations and have a maximum amount specified by law. In contrast, administrative penalties are reserved for more serious violations, with the maximum amount determined as a percentage of the violator’s revenue.

In practice, administrative fines are calculated based on a predetermined amount according to the type and number of violations. These fines can be adjusted – either increased or decreased – by considering factors such as the severity, duration, motive and damage caused by the violation, as well as other legal criteria. Generally, administrative penalties cannot exceed 3% of the violator’s total revenue, although revenue unrelated to the violation is to be excluded from this calculation. Administrative penalties may also be adjusted based on factors such as the number and duration of violations, the profits gained, voluntary corrective actions and efforts to mitigate damage.

Previously, the maximum base amount for administrative penalties was set at “no more than 3% of the revenue related to the violation”. However, with the

implementation of the amended PIPA in 2023, this base amount was changed to “no more than 3% of the total revenue”, while allowing for the exclusion of unrelated revenues. Consequently, with the burden of proving the irrelevance to the violation shifting to the data controller, the amounts of imposed administrative penalties have been increasing.

1.9 Enforcement Trends

The following are key regulatory actions taken by the PIPC from 2024 to 2025. As regulations have recently been strengthened, it is important to proactively assess potential legal violation risks and identify conduct that may be problematic for effective risk management.

In May 2024, the PIPC imposed an administrative penalty of approximately KRW7.5 billion and an administrative fine of KRW5.4 million in a case where personal information of over 2.21 million users was leaked. Additionally, an administrative penalty of approximately KRW15.1 billion and an administrative fine of KRW7.8 million were imposed in a case involving leaks of anonymous chatroom users’ information.

Additionally, in August 2025, the PIPC imposed an administrative penalty of approximately KRW134.7 billion and an administrative fine of KRW9.6 million to a telecommunications carrier in a case where personal information of over 23 million users was leaked. This case marked the largest monetary penalty ever imposed for a personal information leak by the PIPC.

In July 2024, the PIPC fined a Chinese e-commerce service provider an administrative penalty of approximately KRW2 billion and an administrative fine of KRW7.8 million for failing to secure user consent for overseas transfers of personal information and not including necessary data protection measures in seller agreements. This case highlighted that overseas providers are subject to the level of regulation required of domestic service providers to ensure robust protections for managing personal information.

In November 2025, despite repeated requests from the PIPC to submit materials for an investigation, an online wiki operator refused to comply on the grounds

that its headquarters were located overseas and that it was therefore not subject to Korean law. As a result, the PIPC referred the foreign operator to law enforcement authorities.

2. Privacy Litigation

2.1 Privacy Litigation Overview

The administrative penalty amount imposed for violations of the PIPA has increased significantly, and the number of administrative lawsuits filed against the PIPC has been increasing – KRW61.1 billion/three cases in 2024 to KRW167.4 billion/seven cases in 2025 (up to November). Moreover, as explained in **1.8 Enforcement Proceedings and Fines**, the amendment to the PIPA has changed the threshold for administrative penalties, which is expected to further increase the number of administrative lawsuits filed against the PIPC.

In contrast, civil lawsuits brought by data subjects against data controllers most often arise in connection with data breaches, where claims for damages or compensation for mental suffering are pursued. In practice, however, data subjects frequently face difficulties in proving actual financial loss and therefore tend to focus their claims on compensation for mental suffering.

Under the PIPA, data subjects may claim statutory damages of up to KRW3 million even without demonstrating an actual financial harm. In awarding damages, Korean courts consider factors such as the sensitivity of personal information involved, the scale of the breach, and the data controller’s response to the incident. To avoid liability, the data controller must prove that the breach was not caused by intent or negligence, but this burden is often difficult to meet in practice.

2.2 Recent Case Law

Major lawsuits related to privacy in 2025 were as follows.

In 2022, the PIPC imposed an administrative penalty of around KRW100 billion in total to two online platforms on the ground that they did not obtain legiti-

mate consent from users for processing their personal information for personalised advertising purposes. The two online platforms have filed a lawsuit seeking revocation of the disposition imposed by the PIPC. In January 2025, the Seoul Administrative Court dismissed the claims of the two online platforms, though they have appealed to the Seoul High Court. As regulations on the collection of behavioural data and the use of personalised advertising are being tightened in other jurisdictions such as the EU, this case is the first decision in Korea regarding the collection and use of behavioural data on personalised online advertising platforms, drawing keen attention to the outcome of the court's further decision.

In 2025, the Supreme Court held that, depending on the circumstances, submitting litigation documents or evidence containing personal information to a court to substantiate claims or to defend against criminal charges, and submitting evidentiary materials containing personal information to law enforcement authorities in connection with criminal complaints or investigations to substantiate allegations or to exercise the right of defence, may constitute “justifiable acts” under the Criminal Code – and therefore would not be punishable as violations of the PIPA. Previously, because the PIPA contained no explicit provision authorising the submission of documents containing personal information to courts or law enforcement authorities without a warrant or court order, such conduct had been regarded as potentially constituting a violation of the PIPA. However, following the Supreme Court's ruling, the legal risk associated with such submissions has been reduced.

In 2025, the Supreme Court held that a data subject's right under the PIPA to request the suspension of personal information processing does not extend to pseudonymisation of personal information. The case arose when mobile subscribers sought to suspend the pseudonymisation of their personal information, which was being carried out for purposes of scientific research, statistical analysis, and the preservation of records in the public interest. Mobile service providers refused the request, and the dispute proceeded to litigation. In reaching this conclusion, the Supreme Court emphasised that the PIPA clearly distinguishes between “processing” and “pseudonymisation”,

and reasoned that pseudonymisation is a method designed to reduce the risk of individual identification and is, therefore, different in nature from ordinary processing of personal information. The Court further noted that the legislative intent underlying the PIPA provision on pseudonymisation was to promote data utilisation and foster new industries.

In 2025, the Supreme Court issued a decision adopting a broader interpretation of the scope of “use” of personal information under the PIPA. The case involved a daycare centre director, the defendant, who reviewed CCTV footage recorded at the daycare centre to check whether teachers were using their mobile phones during working hours, and then orally communicated information about such mobile phone use based on what was observed from the footage. The key issue in this case was whether conveying information obtained from the CCTV footage, rather than providing the footage itself, constituted a “use” of personal information beyond the original purpose for which the information was collected. The Supreme Court held that the “use” of personal information is not limited to using the data in its originally collected form, but also includes processing, editing or extracting information from the collected personal information and the subsequent use of the resulting information. On this basis, the Supreme Court concluded that the defendant had used the personal information beyond the scope of the original purpose for which it was collected, in violation of the PIPA.

2.3 Collective Redress Mechanisms

The PIPA includes a mechanism for collective redress through a dispute mediation system. This allows national and local governments, personal information protection organisations, data subjects and data controllers to request or apply for collective dispute mediation via the Dispute Mediation Committee. This process is applicable in situations where multiple data subjects experience similar damage or rights infringements, provided the following criteria are met.

- At least 50 data subjects must have suffered harm, excluding:
 - (a) data subjects who have already reached an agreement with the data controller regarding dispute resolution or compensation;

- (b) individuals who are currently involved in a dispute mediation process under different laws or regulations for the same issue; and
- (c) individuals who have filed a lawsuit regarding the personal information infringement in question.
- The case's key issues must share common factual or legal characteristics.

Despite this framework, collective dispute mediation has been rarely utilised.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

There are no general laws or regulations governing the protection and processing of non-personal data. Instead, such matters are regulated under sector-specific legislation. For instance, in the field of cloud computing, the Cloud Computing Act applies. While the Cloud Computing Act does not prescribe specific provisions on data transfer, it prohibits a cloud service provider, or any third party that has received user information from the provider, from providing such information to another third party or using it for purposes other than service provision without the user's consent, unless required to do so by a court order or a warrant issued by a judge.

Separately, depending on the type of issue, the following individual laws and regulations may apply.

- Security and safety management: the Network Act mandates manufacturers and importers of IoT devices to implement protective measures to ensure the stability and reliability of information and communications networks. Additionally, the Network Act includes an information protection certification system for IoT products.
- Data sharing: there is no law similar to the EU Data Act that directly requires data holders to share data during the development, launch or operation of IoT products. However, the Framework Act on Promotion of Data Industry and Promotion of Use allows the government to support the establishment of data distribution and transaction systems.

- For issues such as wiretapping, Korean law restricts recording and listening to conversations among unspecified individuals. Service providers need to ensure compliance with these restrictions to avoid violations, including under the following:
 - (a) the Protection of Communications Secrets Act – prohibits unauthorised wiretapping and recording of undisclosed conversations;
 - (b) the Network Act – forbids damaging, misappropriating or divulging others' information processed through a communications network; and
 - (c) the Korean Criminal Code – deems it illegal to obtain confidential documents or electronic records through technical means without authorisation.
- Location information: in Korea, the use of location information is governed by the Location Information Act. The Location Information Act is particularly relevant when collecting and using location data.

3.2 Interaction of Data Regulation and Data Protection

Under Korean law, the frameworks mentioned in 3.1 Objectives and Scope of Data Regulation apply concurrently, unless a specific statute expressly excludes the application of another.

For personal information, the PIPA serves as the general law. In cases where a more specific statute governs a particular type of personal information, that statute prevails over the PIPA under the *lex specialis* principle. For instance, as a special law for location information, the Location Information Act takes precedence over the PIPA for location information.

3.3 Rights and Obligations Under Applicable Data Regulation

Unlike personal information, which entails specific legal rights and obligations under the PIPA, non-personal information faces lighter regulation, unless such non-personal information falls into special categories (eg, state secrets). For instance, data subjects whose personal information is processed may exercise the data subject's rights under the PIPA, such as access and data portability, and data controllers must respond promptly.

By contrast, for non-personal information, there are no general laws or regulations that grant similar rights or obligations. For example, although public institutions are generally required to disclose most of their data for free use (with some exceptions), this requirement does not extend to private companies. Also, the government may recommend that cloud service providers establish co-operation frameworks to promote interoperability, though such recommendations are not legally binding. Therefore, companies should distinguish personal information from non-personal information and tailor compliance efforts accordingly.

3.4 Regulators and Enforcement

As explained in **1.7 Regulators**, the key regulatory authorities include the PIPC, KMCC, KISA, FSC and MSIT. If multiple laws apply to a given matter, these regulators may exercise regulatory authority concurrently. For instance, as noted in **1.6 Data Breach Requirement**, recent cases have involved simultaneous investigations by the PIPC, KISA and MSIT's joint private-public task force into cyber-incident and data breaches.

4. Sectoral Topics

4.1 Use of Cookies

The PIPA does not require data controllers to obtain users' consent for the installation of cookies, nor does it restrict the use of cookies. However, if the information collected through cookies qualifies as personal information – defined by the PIPA as information that can be easily combined with other information to identify an individual – it falls under the PIPA's regulations, and legal basis such as explicit opt-in consent is required. The PIPA also obligates data controllers to state “matters concerning the installation, operation and refusal of a device that automatically collects personal information, such as an internet access data file” in their privacy policies – ie, data controllers are obligated to state such matters when installing and operating a device that automatically collects personal information such as a cookie or similar technology on their own web or app.

Please refer to **4.2 Personalised Advertising and Other Online Marketing Practices** for enforcement

trends related to behavioural information collected through cookies.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised Advertising

In the absence of specific statutory regulations regarding the processing of behavioural data for personalised advertising, the general legal principles of the PIPA apply if such information is considered personal information. That is, if online identifiers used for targeted advertising, along with the behavioural information collected, can be combined to personally identify individuals, this information is classified as personal information. Consequently, to collect and use this behavioural data for personalised advertising, the legal requirements for processing personal information – such as securing legitimate legal grounds for processing – must be met.

Conversely, if the behavioural data does not enable the identification of specific users, it is not considered personal information under the PIPA. In this scenario, PIPA regulations do not apply, though the PIPC recommends implementing safety measures.

Online Marketing Practices

In order to send marketing communications via an electronic medium such as email or SMS, data controllers must obtain from the data subject:

- consent to processing their personal information for marketing purposes pursuant to the PIPA; and
- consent to receiving marketing communications in accordance with the Network Act.

Data controllers are required to comply with certain formality requirements to clearly show that the information is an advertisement, and separate consent from the data subject is required for night-time transmission.

Children's Data

As explained in **1.3 Special Categories of Personal Data**, the PIPA generally requires data controllers to obtain consent from a legal guardian when obtaining consent for processing personal information of children under 14. Moreover, when providing notices

to such children under the age of 14, data controllers must use simple and clear language and formats. Separately, the “Guidelines to Protection of Children and Youth Personal Information (December 2024)” published by the PIPC require minimising targeted ads based on children’s behavioural data, providing clear prior notice and obtaining consent. If data controllers serve targeted ads by combining behavioural data and personal information of children under 14, they must obtain prior consent from the child’s legal guardian.

4.3 Employment Privacy Law

There are no specific regulations or considerations exclusively for processing employees’ personal information; instead, the general provisions of the PIPA apply. The PIPC’s “Guidelines for Protection of Personal Information by Field (December 2024)”, under the “HR/Labour” section, provides some guidance on processing personal information related to hiring and employment. Key details include the following.

Processing Employee Data in a Job Application Context

Under the Hiring Procedures Act, employers may collect only the personal information strictly necessary for hiring, and must not collect information unrelated to job duties. They may process such minimal information without the applicant’s consent, but they must obtain explicit consent before collecting sensitive information or unique identification information. If collecting sensitive information or unique identification information is unavoidable, employers must obtain separate consent from the applicant.

Criminal Background

Under the Act on the Lapse of Criminal Sentences, employers are restricted to a certain extent when collecting applicants’ criminal records.

Monitoring of Employees

When the legal basis for collecting and using employees’ personal information for monitoring purposes is unclear, employers must obtain the employees’ consent. In such cases, employers must ensure truly voluntary consent, considering the inherent imbalance in labour-management relations.

Surveillance Devices

Installing surveillance devices, such as CCTV, in the workplace requires labour-management consultation according to the Act on the Promotion of Workers’ Participation and Co-Operation. Employers must not use CCTV audio recording functions and are required to install signboards (or equivalent notices) disclosing the fact of filming and its scope.

Data Retention

Employers must retain employee data for a specific period as mandated by the Labour Standards Act.

Transparency

Employers must include details of employees’ personal information processing in their privacy policy and make it easily accessible to employees.

Also, in terms of sharing employees’ personal information with affiliates outside Korea, data controllers must pay close attention to the legal requirements explained in **5.1 Restrictions on International Data Transfers**.

4.4 Data Protection in M&A

Regarding data protection in M&A, general principles and regulations of the PIPA apply. For example, data transfer to third parties, as detailed in **5.1 Restrictions on International Data Transfers**, typically involves either third-party provision or delegation of processing. Transferring personal information in the course of M&A is likely to be considered as third-party provision.

While the PIPA generally requires consent from data subjects to provide personal information to a third party, it includes a specific provision regarding the transfer of personal data during asset deals. If a data controller transfers personal information as part of a business transfer or a merger involving all or part of its operations, the controller must notify the data subjects in advance about the following, and a consent requirement is exempted:

- the fact that their personal information will be transferred;
- the name, address, telephone number and other contact information of the recipient of the personal information; and

- the method and procedure for withdrawing consent if the data subject does not wish their personal information to be transferred.

In principle, the business transferor must provide the above information in writing (eg, written document, email, fax, phone, text message or any other equivalent method). However, if the business transferor is unable to provide such information in writing without negligence, the business transferor must publish this information on a website for at least 30 days. If there is a justifiable reason for not being able to publish the above information on a website, the business transferor must:

- publish the above information in an easily visible location within the business transferor's place of business for at least 30 days; or
- publish it in a daily newspaper that is mainly distributed in the city, province or region where the business transferor's place of business is located.

The business transferee has the same notification obligation as the business transferor. However, if the notification has been provided by the business transferor, the business transferee is not required to provide one. Meanwhile, a business transferee that has received personal information as part of a business transfer or merger may use the personal information or provide it to a third party only for the original purpose for which it received the information.

5. International Considerations

5.1 Restrictions on International Data Transfers

Under the PIPA, a data controller may transfer personal information overseas (ie, provide, delegate the processing of, or store personal information with an overseas entity) only on one or more of the following grounds:

- where the data controller obtains separate consent from the data subject;
- where there is specific authorisation by treaty or other international agreement;

- where personal information is stored overseas and/or personal information processing is delegated to an overseas entity because it is necessary for the execution and performance of an agreement with the data subject, and certain information regarding the overseas transfer (storage/delegation) is disclosed to the data subject, through either the data controller's privacy policy or other written means such as email;
- where the recipient party located overseas has obtained certification from the PIPC, and has taken measures to ensure that personal information and rights of data subjects are protected and to implement the matters subject to certification in the destination country; or
- where the PIPC has recognised the adequacy of the level of the privacy protection provided in the destination country.

In the case of international data transfers, the data controller must consult with the recipient and reflect the following in the relevant agreement:

- measures to ensure safety for protecting personal information under the PIPA;
- measures to handle grievances and resolve disputes with respect to personal information breaches; and
- other measures necessary to protect the personal information of data subjects.

Third-Party Transfers

Separate from such regulation regarding overseas transfers, transferring personal information to a third party outside Korea for the purpose of either providing personal information to a third party or delegating the processing of personal information also constitutes third-party provision or delegation of processing of personal information under the PIPA, respectively – these are subject to the relevant provisions of the PIPA in addition to the above-mentioned regulation on overseas transfer. Third-party provision occurs where a data controller provides personal information to a third-party recipient for the purpose and benefit of the third-party recipient. Delegation occurs where a third-party entity processes personal information that it receives from the data controller for the purpose and benefit of the data controller.

Restrictions on third-party provision and delegation

If the transfer in question constitutes a third-party provision within the original purpose of collection, the PIPA requires the data controller to meet at least one of the following grounds:

- where the data controller obtains consent from the data subject;
- where there are special provisions in law allowing third-party provision, or third-party provision is inevitable to comply with statutory obligations;
- where third-party provision is evidently deemed necessary for urgent protection of life, body or property of a data subject or a third party;
- where third-party provision is necessary to achieve the legitimate interests of a data controller, and such necessity clearly supersedes the rights of the data subject – in such cases, third-party provision is limited to where the legitimate interests of the data controller are substantially related and do not go beyond the reasonable scope; or
- where third-party provision is urgently required for public safety and security.

If the transfer in question constitutes a delegation, consent from the data subject is not required. However, the data controller must disclose details of delegation and enter into a written agreement with the entity that is delegated with the processing of personal information. Such agreement must include matters that are statutorily required under the PIPA.

5.2 Government Notifications and Approvals

Apart from the regulations mentioned in **5.1 Restrictions on International Data Transfers** and **5.3 Data Localisation Requirements**, data controllers are not required to provide notification to government agencies or to obtain approvals.

5.3 Data Localisation Requirements

While there is no general data localisation rule under the PIPA, there are individual laws that prohibit overseas transfer of specific types of data, such as the following:

- the Medical Services Act prohibits storing electronic medical records (EMR) outside Korea;

- the Act on the Establishment and Management of Spatial Data requires a licence to transfer certain map data outside Korea;
- the Industrial Technology Protection Act requires a company to obtain approval from or file a prior report with the Ministry of Trade, Industry and Energy in order to export national core technology;
- the Electronic Financial Transactions Act stipulates that financial companies or electronic financial business operators' systems for processing unique identification information or personal credit information cannot be located outside Korea in the course of using cloud computing services; and
- the Cloud Computing Act stipulates that data processed by Korean government organisations and public institutions must be located in Korea.

5.4 Blocking Statutes

There are no “blocking” statutes that protect Korean companies from the effect of extraterritorial sanctions.

5.5 Recent Developments

As outlined in **5.1 Restrictions on International Data Transfers**, one of the legal bases for transferring personal information internationally is when the PIPC acknowledges that the destination country provides an adequate level of privacy protection. In September 2025, the PIPC announced its first adequacy decision for the EU as well as its plans to expand this to countries such as the UK and Japan through future adequacy review. For countries such as the USA, where privacy frameworks differ significantly despite high data transfer needs, the PIPC plans to develop customised overseas transfer mechanisms.

Moreover, the PIPC plans to broaden the available mechanisms for the secure and seamless overseas transfer of personal information by amending the PIPA in the first half of 2026. These mechanisms may include the Standard Contractual Clauses prepared by the PIPC or Binding Corporate Rules of multinational companies approved by the PIPC. The PIPC also plans to introduce the Overseas Transfer Impact Assessment System for self-evaluating risks in large-scale overseas transfers of highly sensitive data, alongside an Overseas Transfer Pre-Review System tailored for M&A activities.

Trends and Developments

Contributed by:

Hwan Kyoung Ko, Sunghee Chae, Kyung Min Son and Matt Younghoon Mok
Lee & Ko

Lee & Ko was established in 1977 and has evolved into a leading full-service law firm in South Korea, recognised for its excellence across various legal domains. Lee & Ko is known for delivering timely, practical solutions in complex legal matters. The firm's in-house resources include attorneys, accountants, patent agents, former government officials and other specialists, ensuring that clients can access a wide

range of services cost-effectively. Further, Lee & Ko maintains an extensive global network and collaborates with international law firms. This allows the firm to assist clients not only with Korean legal matters but also with cross-border transactions by connecting to legal advisers worldwide, making the firm a sought-after choice for clients requiring comprehensive and efficient legal assistance.

Authors



Hwan Kyoung Ko is a partner at Lee & Ko and heads the data privacy and cybersecurity team, the tech and AI team, and the platform regulation response team. He is widely recognised as a leading expert in data

protection and cybersecurity in Korea. He has advised major domestic and global companies on high-profile data breach investigations, regulatory proceedings and enterprise-wide data governance projects. He also advised on amendments to the Personal Information Protection Act and the Credit Information Act. Mr Ko serves as Vice-Chairman of the Korea Personal Information Protection Law Association, and is a member of several government AI and data policy committees.



Kyung Min Son joined Lee & Ko in 2011 and has since specialised in data protection and privacy law, advising domestic and international IT companies and financial institutions on a wide range of personal

information matters. He represents clients in investigations by the Personal Information Protection Commission, and handles administrative sanctions and related litigation. He also advises on data breaches, cybersecurity incidents and data subject rights issues. Mr Son has extensive experience in leading data protection compliance projects and providing regulatory consulting. His practice further includes advising on data protection issues in M&A transactions, location-based services regulation, and healthcare data matters.



Sunghee Chae has focused her practice at Lee & Ko on privacy and data protection since 2016. She advises Korean and multinational clients across the technology, finance, healthcare, manufacturing and

mobility sectors on complex regulatory and data governance matters. Her experience includes developing and implementing global privacy compliance programmes and cross-border data transfer strategies, as well as addressing data protection issues related to digital services and emerging technologies. She also counsels clients on regulatory investigations, data security incidents, workforce privacy and evolving cybersecurity compliance requirements.



Matt Younghoon Mok is a senior foreign attorney in Lee & Ko's TMT group, where he focuses on data privacy, cybersecurity, artificial intelligence, and emerging technology regulations. His expertise spans

cryptocurrency compliance, blockchain technology and cross-border transactions. In addition to his technical focus, Mr Mok has significant experience in advising on corporate matters, including M&A, joint ventures and other transactional work. He is admitted to practice in the District of Columbia.

Lee & Ko

Hanjin Building
63 Namdaemun-ro
Jung-gu
Seoul 04532
South Korea

Tel: +82 2 772 4000
Fax: +82 2 772 4001 2
Email: mail@leeko.com
Web: www.leeko.com



Korea's 2026 Amendments to the Personal Information Protection Act: Strengthened Corporate Accountability and Developments in AI-Related Data Use

Introduction

In 2025, Korea experienced a series of unprecedented large-scale personal data breaches across sectors closely connected to everyday life, including telecommunications, e-commerce and financial services. A major telecommunications company, SK Telecom, suffered a hacking incident affecting approximately 23 million users. An e-commerce platform, Coupang, reported the exposure of approximately 33 million customer records, and a credit card company, Lotte-Card, experienced a breach involving approximately 2.97 million individuals. These cross-sector incidents revealed significant weaknesses in corporate data protection governance.

The regulatory response was substantial. While the investigations by the Personal Information Protection Commission (PIPC) concerning Coupang and Lotte-Card remain ongoing, the PIPC imposed an administrative penalty exceeding KRW134.7 billion (approximately USD93 million) in relation to the SK Telecom data breach. More recently, it imposed administrative penalties totalling KRW36.033 billion (approximately USD25 million) against Korean subsidiaries of Louis Vuitton, Dior and Tiffany & Co for personal data breach. These enforcement actions underscored that inadequate data protection systems may give rise to significant regulatory, commercial and reputational exposure.

The recurrence of large-scale breaches prompted criticism that existing corporate governance and internal control mechanisms were insufficient to prevent systemic data protection failures. In response, the National Assembly pursued legislative reform aimed at strengthening accountability and enhancing the effectiveness of the Personal Information Protection Act (PIPA).

On 12 February 2026, the National Assembly passed a bill partially amending the PIPA (the "Amended PIPA"). The amendments extend beyond increasing administrative penalties and instead revise core elements of the statutory framework. Key changes include:

- express clarification of the responsibility of representative directors;
- strengthened authority and reporting functions of the Chief Privacy Officer (CPO);
- mandatory Personal Information and Information Security Management System (ISMS-P) certification for data controllers meeting prescribed thresholds;
- restructuring of the personal data breach notification regime;
- introduction of an aggravated administrative penalty of up to 10% of total turnover for repeated or serious violations; and
- revision of administrative fine provisions.

Through these measures, the Amended PIPA clarifies that personal data protection is not limited to technical compliance obligations but forms part of corporate management and governance responsibility. The

Amended PIPA will enter into force six months after promulgation, though the mandatory ISMS-P certification requirements will take effect from 1 July 2027.

In parallel with the strengthening of corporate responsibility, the PIPC has also indicated its intention to introduce special statutory provisions permitting limited processing of personal data for artificial intelligence (AI) development or performance improvement, subject to defined conditions and regulatory oversight.

In addition, several significant court decisions have recently been rendered addressing the scope of corporate liability for damages arising from data breaches and the applicability of the right to request suspension of processing in the context of pseudonymisation.

The principal elements of these developments are discussed below.

Key Amendments Under the Amended PIPA *Express clarification of representative director responsibility and strengthening of the CPO's role*

A key structural change introduced by the Amended PIPA concerns the clarification of responsibility for personal data protection within the corporate structure. The amendments expressly identify the representative director (or business owner in the case of a sole proprietorship) as bearing ultimate responsibility, expand the organisational and reporting functions of the CPO, and, for entities meeting prescribed thresholds, subject the appointment and removal of the CPO to board approval and notification to the PIPC. Accordingly, personal data protection in Korea is addressed within formal corporate governance processes rather than solely as an operational compliance matter.

Express clarification of representative director responsibility (new Article 30-3)

The Amended PIPA introduces a new Article 30-3, which expressly provides that a representative director or business owner bears ultimate responsibility for the safe processing of personal data and the protection of data subjects' rights. The provision further requires that such representative director or business owner implement effective overall management measures, including the provision of professional personnel and

sufficient budgetary support necessary for personal data protection.

Expansion of the CPO's duties (Article 31, paragraph 4, subparagraphs 2 and 3)

Article 31 of the Amended PIPA expands the statutory duties of the CPO. In addition to existing responsibilities, the CPO is now required to:

- manage professional personnel necessary for personal data protection and secure the relevant budget; and
- report to the business owner or representative director, as well as to the board of directors, on the status of personal data protection and other major related matters.

Board resolution and reporting obligations for CPO appointment (Article 31, paragraph 3, subparagraphs 1 and 2)

Under the Amended PIPA, data controllers meeting thresholds to be prescribed by Enforcement Decree and based on factors such as turnover and scale of personal data processing are subject to additional procedural requirements concerning the CPO. For such entities:

- the appointment, replacement or dismissal of the CPO must be approved by a resolution of the board of directors; and
- such appointment, replacement or dismissal must be reported to the PIPC.

Mandatory personal information protection certification (ISMS-P)

The Amended PIPA introduces mandatory ISMS-P certification requirements for certain data controllers.

ISMS-P builds upon the existing ISMS certification framework required for certain entities under the Act on Promotion of Information and Communications Network Utilisation and Information Protection, by incorporating additional requirements relating to personal data protection.

Certification is conducted by the Korea Internet & Security Agency (KISA) and, in the case of financial institutions, the Financial Security Institute (FSI), which

evaluate whether an organisation has systematically established and operates measures and activities for information security and personal data protection.

Under the previous regime, obtaining ISMS-P certification was generally voluntary for most data controllers and was often pursued to enhance external credibility regarding the robustness of their data protection practices.

By contrast, the Amended PIPA now requires data controllers meeting prescribed thresholds to obtain ISMS-P certification as a statutory obligation. The applicable thresholds will be determined by Enforcement Decree, taking into account factors such as turnover and the scale of personal data processing. The PIPC has also indicated that it may actively consider revocation of ISMS-P certification in cases involving serious violations relating to personal data protection.

Restructuring of the personal data breach notification regime

The Amended PIPA revises the notification regime applicable to personal data breaches by expanding the scope of personal data breaches subject to notification and broadening the content of required notifications. These changes affect both the timing and scope of notification obligations imposed on data controllers.

Expansion of the scope of personal data breaches subject to notification (Article 23, paragraph 2 and Article 34, paragraph 1)

Before the Amended PIPA, notification to data subjects was required where breached personal data had been “lost, stolen or leaked”. The Amended PIPA expands the scope of personal data breaches to include cases of “forgery, alteration or damage” to personal data.

Introduction of notification obligation in cases of potential personal data breach (Article 34, paragraph 2)

The Amended PIPA introduces a new obligation to notify data subjects even where an actual personal data breach has not yet been conclusively confirmed. Where a data controller becomes aware of a possibility of a personal data breach – as determined under

Enforcement Decree with reference to the type of personal data involved, the potential impact on data subjects and the level of risk – the data controller must, without delay, notify all affected data subjects of such possibility and provide information necessary to minimise harm.

Expansion of notification content (Article 34, paragraph 1)

In addition to the existing notification items required, the Amended PIPA further requires data controllers to inform data subjects of:

- information concerning their legal rights and available methods of exercising such rights, including claims for damages and statutory damages arising from the personal data breach; and
- other matters to be prescribed by Enforcement Decree.

Introduction of an aggravated administrative penalty regime of up to 10% of total turnover

The Amended PIPA revises the administrative penalty framework by introducing an aggravated penalty of up to 10% of total turnover in specified cases of repeated or serious violations, while also establishing a statutory basis for mandatory mitigation in certain circumstances.

Introduction of an aggravated administrative penalty of up to 10% of the total turnover (Article 64-2, paragraph 2)

Under Article 64-2, paragraph 1 of the PIPA, where a violation subject to an administrative penalty occurred, the PIPC was authorised to impose an administrative penalty of up to 3% of the total turnover, excluding turnover unrelated to the violation. Where turnover was absent or difficult to calculate, the maximum administrative penalty was KRW2 billion (approximately USD1.4 million).

The Amended PIPA introduces Article 64-2, paragraph 2, pursuant to which an administrative penalty of up to 10% of the relevant total turnover, excluding turnover unrelated to the violation, may be imposed, or up to KRW5 billion (approximately USD3.5 million) where turnover is absent or difficult to calculate, in the following circumstances:

- where, within three years from the date of a prior administrative penalty, the data controller commits the same type of violation, provided that each violation involves intent or gross negligence (for clarity, the assessment of intent or gross negligence for purposes of administrative penalties follows the criteria specified in the PIPC's administrative penalty guidelines, rather than general Civil Code standards);
- where a violation subject to an administrative penalty is committed with intent or gross negligence and affects more than ten million data subjects; or
- where personal data breach occurs due to failure to comply with a corrective order.

The violations listed in Article 64-2, paragraph 1 – including personal data breach, use or provision of personal data beyond the permitted purpose, and unlawful processing of unique identification information or sensitive information – may fall within the aggravated regime if the above conditions are met.

Introduction of a mitigation provision (Article 64-2, paragraph 6)

The Amended PIPA further introduces Article 64-2, paragraph 6, which provides that an administrative penalty must be reduced where the data controller has made investments and operated measures relating to personal data protection, including budget, personnel, facilities or systems, as prescribed by Enforcement Decree. This mitigation provision does not apply in cases involving intent or gross negligence.

Revision of administrative fine provisions (Article 75)

The Amended PIPA revises and supplements administrative fine provisions in order to ensure the enforceability of newly introduced or amended obligations.

In particular, the following violations are now subject to administrative fines or increased administrative fine amounts:

- failure to designate a CPO, or designation of a CPO who does not meet statutory qualification requirements, with the maximum administrative fine increased from KRW10 million to KRW30 million (approximately USD21,000);

- failure to obtain board approval for the appointment, replacement or dismissal of a CPO, where required, subject to a maximum administrative fine of KRW30 million (approximately USD21,000);
- failure to report the appointment, replacement or dismissal of a CPO to the PIPC, where required, subject to a maximum administrative fine of KRW30 million (approximately USD21,000); and
- failure to obtain mandatory personal data protection certification, subject to a maximum administrative fine of KRW30 million (approximately USD21,000).

Legislative Developments Concerning Special Provisions for AI

Alongside the strengthening of corporate accountability under the Amended PIPA, legislative discussions have progressed regarding the introduction of special provisions permitting certain processing of personal data for AI development or performance improvement. The PIPC has stated, including in its 2026 policy plan, that it intends to complete legislative measures introducing such provisions as part of broader governmental efforts to facilitate the availability of training data and promote AI-driven innovation.

A bill currently pending before the National Assembly proposes to allow, under limited conditions, the processing of lawfully collected personal data beyond the original purpose of collection for AI development or performance improvement. Under the proposed framework, personal data may be utilised in its original form without pseudonymisation or anonymisation, subject to statutory requirements.

Processing beyond the original purpose would, in principle, require deliberation and resolution by the PIPC. Such processing would be permitted only where:

- anonymisation or pseudonymisation alone would make AI development or performance improvement difficult;
- appropriate technical, administrative and physical safeguards are implemented; and
- the processing contributes to public or social interests while presenting a demonstrably low risk of unjust infringement of the interests of data subjects or third parties.

Where personal data is processed pursuant to PIPC deliberation and resolution, the data controller would be required to disclose relevant information in its privacy policy. The PIPC would retain supervisory authority and may restrict all or part of the processing where statutory conditions are not satisfied.

As the bill remains subject to the legislative process, its final content may be amended.

Recent Judicial Decisions

Recent court decisions have clarified key interpretative issues under the PIPA, including the availability of statutory damages following data breaches and the applicability of the right to request suspension of processing in the context of pseudonymisation.

Supreme Court decision on statutory damages (decided 4 December 2025)

The Supreme Court recently clarified that Article 39-2 of the PIPA, which permits statutory damages of up to KRW3 million (approximately USD2,100) without detailed proof of actual loss in cases of personal data breach, does not automatically require compensation solely because a breach has occurred and that at least the occurrence of compensable mental harm (not so much of the volume or severity of such harm) must be proved by the plaintiffs.

The case concerned a hacking incident affecting approximately 400,000 users of an online knowledge-sharing platform and involving encrypted passwords and email addresses. The plaintiffs asserted that the external leakage of their encrypted passwords and email addresses caused mental harm and sought compensation under Article 39-2 against the platform operator.

The Court held that Article 39-2 does not mandate compensation in all personal data breach cases and clarified that the provision is not intended to impose liability where it is clear that no compensable damage has arisen. Accordingly, where a data controller demonstrates that no mental or other legally compensable harm warranting damages has occurred, liability for statutory damages may be denied.

In reaching this conclusion, the Court considered (among other factors) that:

- the leaked passwords were encrypted, significantly reducing the likelihood that third parties could identify or misuse them;
- the email addresses were not leaked in combination with other identifying personal data and were not readily sufficient, by themselves, to identify specific individuals; and
- given the nature of the knowledge-sharing platform, the leaked email addresses alone were unlikely to reveal users' characteristics or preferences.

On that basis, the Court concluded that the risk of infringement of privacy, reputation or property interests was low and that it was difficult to recognise the occurrence of compensable mental harm.

Supreme Court decision on pseudonymisation and the right to request suspension (decided 18 July 2025)

The Supreme Court addressed whether a pseudonymisation process conducted pursuant to Article 28-2 of the PIPA for purposes such as statistical compilation, scientific research or archiving in the public interest constitutes "processing" subject to the right to request suspension under Article 37, paragraph 1.

Article 28-7 expressly excludes the application of Article 37 to "pseudonymised data" prepared in accordance with Article 28-2. The dispute in this case concerned an earlier stage: whether the pseudonymisation process itself falls within the meaning of "processing of personal data" under Article 37, paragraph 1. If the plaintiffs' interpretation was accepted, data subjects could request suspension of pseudonymisation at the processing stage, potentially affecting the practical operation of the statutory pseudonymisation framework introduced to facilitate data utilisation, including for AI development.

Lower courts had concluded that the pseudonymisation process fell within the statutory definition of "processing", which includes collection, use, provision and other handling of personal data, and there-

fore held that data subjects could request suspension of such pseudonymisation.

The Supreme Court accepted the defendant's position and reversed the lower courts' decisions. It reasoned that pseudonymisation under Article 28-2, which involves deleting or replacing part of personal data so that individuals cannot be identified without additional information, functions as a protective measure designed to reduce identification risk. In light of its legislative purpose and structure, the Court held that pseudonymisation carried out pursuant to Article 28-2 does not fall within the scope of "processing" subject to the right to request suspension under Article 37, paragraph 1. On remand, the appellate court subsequently followed the Supreme Court's reasoning, thereby confirming the interpretative approach adopted by the Supreme Court.

This decision, rendered in proceedings in which the defendant was represented by Lee & Ko, has attracted considerable attention in academic and industry circles. By clarifying that pseudonymised data may be utilised, including for purposes such as AI training, without being subject to suspension requests, the ruling is widely regarded as having materially strengthened the legal foundation for data-driven innovation in Korea.

Implications and Outlook

The 2026 amendments to the PIPA reflect a clear shift towards strengthening corporate accountability for personal data protection at the governance level. By expressly identifying representative directors as ultimately responsible, expanding the statutory duties and reporting lines of CPOs to the representative director and board of directors, mandating certification for certain data controllers and introducing an aggravated administrative penalty regime of up to 10% of total turnover in specified cases, the Amended PIPA reinforces that personal data protection is a matter of board-level oversight rather than solely operational compliance.

In this environment, establishing or reinforcing an effective internal governance framework for personal data protection will become an urgent priority. This includes ensuring sufficient investment in personnel, systems and facilities, as well as reviewing internal policies and organisational roles relating to data protection. Given that such measures may require amendments to internal regulations or adjustments to cross-functional responsibilities, prudent preparation aligned with the Amended PIPA is advised.

Recent judicial decisions have clarified important boundaries of liability. While the Supreme Court has confirmed that statutory damages are not automatically awarded in all leakage cases, civil claims for statutory or compensatory damages are expected to continue following data breach incidents. In responding to such claims, careful legal analysis of the nature of the leaked information, the likelihood of combination with other data, the risk of secondary harm and the adequacy of post-incident remedial measures will be critical.

At the same time, legislative discussions concerning AI-related data processing signal an effort to balance data protection with data utilisation. Taken together, these regulatory and judicial developments suggest that organisations operating in Korea should approach personal data protection as an integrated governance, compliance and risk management issue in an evolving regulatory landscape.

SWEDEN



Law and Practice

Contributed by:

Anna Fernqvist Svensson, Karl-Fredrik Björklund and Jakob Westling
Hellström Advokatbyrå KB

Contents

1. Legal and Regulatory Framework p.455

- 1.1 Overview of Data and Privacy-Related Laws p.455
- 1.2 Rights and Obligations p.456
- 1.3 Special Categories of Personal Data p.457
- 1.4 Processing of Personal Data for Research and Development Purposes p.457
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.458
- 1.6 Data Breach Requirement p.459
- 1.7 Regulators p.459
- 1.8 Enforcement Proceedings and Fines p.460
- 1.9 Enforcement Trends p.460

2. Privacy Litigation p.461

- 2.1 Privacy Litigation Overview p.461
- 2.2 Recent Case Law p.461
- 2.3 Collective Redress Mechanisms p.461

3. Requirements for the Protection and Processing of Non-Personal Data p.461

- 3.1 Objectives and Scope of Data Regulation p.461
- 3.2 Interaction of Data Regulation and Data Protection p.462
- 3.3 Rights and Obligations Under Applicable Data Regulation p.462
- 3.4 Regulators and Enforcement p.463

4. Sectoral Topics p.463

- 4.1 Use of Cookies p.463
- 4.2 Personalised Advertising and Other Online Marketing Practices p.464
- 4.3 Employment Privacy Law p.464
- 4.4 Data Protection in M&A p.465

5. International Considerations p.465

- 5.1 Restrictions on International Data Transfers p.465
- 5.2 Government Notifications and Approvals p.466
- 5.3 Data Localisation Requirements p.467
- 5.4 Blocking Statutes p.468
- 5.5 Recent Developments p.468

Hellström Advokatbyrå KB was founded in 1991, and has established itself as one of Sweden's most respected commercial law firms through its ability to identify innovative solutions and deliver comprehensive legal support. Hellström is a full-service firm. The firm serves listed companies, SMEs, municipalities, county councils and organisations, delivering tailored solutions within the field of data protection law, including compliance analyses, policy development, contractual documentation and incident management. Services encompass both long-term strategic GDPR implementation and complex, specific legal

issues. With a client-centred approach, Hellström combines deep legal expertise with a practical understanding of the commercial realities its clients face, ensuring advice that is not only legally sound but also operationally effective. The firm also provides training programmes for employees, management teams and boards to ensure comprehensive understanding of data protection obligations and best practices. The firm is engaged in several international legal networks. Hellström is a collaborating firm of US-based Andersen.

Authors



Anna Fernqvist Svensson is a partner at Hellström Advokatbyrå KB, and heads the firm's Data Protection Team. With more than 20 years of experience in data protection, she provides legal advice on complex

data protection matters. Client assignments include acting as DPO, assisting DPOs in their daily work, drafting DPIAs, assessments of third-country transfers, camera surveillance, personal data breaches, AI, whistle-blowing, and dispute resolution. Anna advises clients within the industries of real estate, IT, retail, energy, transport, and pharmaceuticals both within the private and the public sector. She is an experienced lecturer. Anna is a member of Andersen's IT, IP and Data Protection service line.



Jakob Westling specialises in data protection law (GDPR) and employment law with particular expertise in online digital advertising and privacy compliance. He brings valuable regulatory insight from his

previous experience at the Swedish Authority for Privacy Protection and the Stockholm Administrative Court, providing clients with a deep understanding of enforcement perspectives and administrative processes.



Karl-Fredrik Björklund is a distinguished expert in data protection and GDPR compliance, serving as Data Protection Officer and adviser to major organisations, including government authorities. He

possesses extensive experience in complex commercial IT agreements, outsourcing arrangements and system deliveries, as well as commercial dispute resolution in court and arbitration proceedings. Karl-Fredrik has served as course leader for the Swedish Authority for Privacy Protection's (IMY) data protection training programmes and is Vice Chairman of the Forum for Data Protection, a professional association dedicated to developing DPO competence. His multidisciplinary expertise spans data protection, IT law, employment law and commercial litigation.

Hellström Advokatbyrå KB

Kungsgatan 33
XV Floor
S-111 57 Stockholm
Sweden

Tel: +46 8 22 09 00
Email: info@hellstromlaw.com
Web: www.hellstromlaw.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Primary Legal Sources

Sweden's data protection regime is built on the GDPR (Regulation (EU) 2016/679), which sets the core rules for processing personal data and is directly applicable in Sweden.

The Swedish Data Protection Act (*lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning*) complements the GDPR by providing national rules permitted under the Regulation.

Ordinance (2018:219) with supplementary provisions to the EU Data Protection Regulation (*förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning*) complements the Swedish Data Protection Act, providing more specific regulations.

Chapter 2, section 6, second paragraph, of the Swedish Constitution (*regeringsformen (1974:152)*) stipulates that everyone is protected against significant infringements of personal privacy by the public authorities if this occurs without consent and involves surveillance or mapping of the individual's personal circumstances. The European Convention on Human Rights (*européiska konventionen om skydd för de mänskliga rättigheterna (lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna*), EKMR), and the Charter of Fundamental Rights of the

European Union (*Europeiska unionens stadga om de grundläggande rättigheterna*) (*EU:s rättighetsstadga*)).

Furthermore, data protection-related questions are found in the Fundamental Law on Freedom of Expression (*yttrandefrihetsgrundlagen (1991:1469)*, YGL), and the Public Access to Information and Secrecy Act (*offentlighets- och sekretesslagen (2009:400)*, OSL), when it relates to the balancing act between freedom of speech and personal integrity.

Sectorial Laws

For criminal matters, the relevant law is the Law Enforcement Data Act (*brottssdatalagen (2018:1177)*).

There are specific laws for surveillance through cameras (the Camera Surveillance Act (*kamerabevakningsslag (2018:1200)*)), and processing of personal data for credit scoring (the Credit Information Act (*kreditupplysningslag (1973:1173)*)).

For the health sector the Patient Data Act (*patientdatalagen (2008:355)*) supplements the GDPR.

Furthermore, several governmental agencies have their own data protection laws regulating the purposes for which personal data can be processed in their own organisation. This includes the Swedish Tax Agency, etc.

Interaction Between Legal Levels

The GDPR takes precedence as directly applicable EU law. Swedish legislation cannot contradict the GDPR but can differentiate when provided by the regulation.

When applying the sectoral legalisation, the legal principle *lex specialis* is applied, meaning the more specific law takes precedence.

To illustrate this by way of example, the European Convention on Human Rights establishes a right to privacy, which is further elaborated upon through the GDPR. The Swedish Data Protection Act then specifies applicable rules where permitted by the GDPR. The Ordinance with supplementary provisions to the EU Data Protection Regulation in turn sets out certain rules relating to the Swedish Data Protection Act.

Extraterritorial Reach

The Swedish Data Protection Act states that data protection laws apply to the processing of personal data carried out within the framework of activities conducted at the establishments of data controllers or data processors in Sweden. The Act also applies to the processing of personal data carried out by data controllers that are not established in Sweden but in a place where Swedish law applies according to international law.

The Act also applies to the processing of personal data carried out by data controllers or data processors that are only established in third countries, if the processing concerns data subjects who are located in Sweden and is related to:

- the offering of goods or services to such data subjects; or
- the monitoring of their behaviour in Sweden.

Interplay with Non-Personal Data, Cyber and AI Laws

The EU AI Act (Regulation (EU) 2024/1689) is directly applicable in Sweden. It supplements the GDPR, it does not replace it. Providers and deployers must still comply with the GDPR where personal data is processed. There are no specific Swedish provisions that alter this interaction beyond what is set out in the EU legislation.

Two key EU instruments govern cybersecurity and intersect with data law more broadly: the NIS2 Directive and the Cyber Resilience Act (CRA). While the GDPR focuses on personal data, NIS2 and the CRA

extend protection to encompass comprehensive cybersecurity requirements more broadly, covering system and product security irrespective of whether the data involved is personal. Organisations can build on their existing GDPR compliance frameworks, particularly in the areas of risk assessment, incident reporting, and security measures.

1.2 Rights and Obligations

General Principles

The Swedish Data Protection Act does not increase the available rights or principles under the GDPR for data subjects; the same rights and principles outlined in the GDPR apply.

However, chapter 8 in the Swedish Patient Data Act covers patient rights regarding medical records, including:

- access to and copying of records upon request;
- procedures when access is denied;
- provisions for record destruction under certain conditions; and
- information rights about data access.

Compliance Checklist

Core GDPR operational tasks typically include:

- mapping processing operations and purposes;
- identifying lawful bases for processing;
- assessing a special category of personal data/ personal data relating to criminal convictions and offences;
- drafting and providing information to data subjects;
- enabling access/rectification/erasure/objection/ portability and limits to automated decisions – ie, data subjects' rights;
- implementing appropriate technical and organisational measures to ensure security of processing;
- maintaining records of processing activities;
- conducting DPIAs for high-risk processing;
- appointing a DPO where required;
- setting processor terms;
- breach readiness/notifications; and
- transfer mechanisms.

National regulation relating to Healthcare Data

Healthcare organisations must:

- ensure that patient journals are maintained with required content and retention;
- enforce internal confidentiality and role-based access with logging and periodic audits;
- enable patient blocking of intra-provider electronic access;
- limit sensitive search keys for special categories of personal data that is not strictly health related;
- use GDPR-compatible legal bases and secrecy for health data; and
- for quality registers, implement opt-out, proper purposes, authority-controller, minimisation and erasure of data (*gallring*).

1.3 Special Categories of Personal Data

General Prohibition and Exceptions

Special categories of personal data are prohibited to process unless certain conditions are fulfilled (eg, explicit consent, employment/social security, vital interests, public interest in health, research with safeguards). Processing requires professional secrecy for healthcare workers in line with Article 9.2.j GDPR. The professional secrecy is outlined in Chapter 6, Section 12, of the Patient Safety Act (2010:659) (*patientsäkerhetslagen* (2010:659)).

Data relating to criminal convictions needs legal control or a legal basis with safeguards to be processed. Chapter 3, Section 8, of the Data Protection Act stipulates that data relating to criminal convictions may always be processed by government agencies. Parties other than government agencies may process data relating to criminal convictions if the processing is necessary to:

- establish, exercise or defend legal claims, or
- fulfil a legal obligation under an Act or Ordinance.

According to IMY's regulations on the processing of personal data concerning criminal offences, IMYFS 2024:1, the following organisations may process criminal data:

- non-public authorities in social services;
- independent schools and private higher education institutions (for student welfare records);
- law firms and other legal service providers;

- companies with internal whistle-blowing channels (for senior personnel investigations);
- companies under the supervision of the Swedish Financial Supervisory Authority (*Finansinspektionen*); and
- companies under the supervision of the Inspectorate of Strategic Products or the Swedish Radiation Safety Authority.

Data Processing Relating to Minors

Under Article 8 GDPR, where consent is the legal basis for processing (Article 6 (1)(a)), the processing of a child's personal data in relation to information society services is lawful only if the child is at least 16 years old. For children below the age of 16, processing is only lawful if consent is given or authorised by the holder of parental responsibility.

Through Chapter 2, Section 4 of the Swedish Data Protection Act, Sweden has exercised its option under Article 8 GDPR to lower the age threshold. When information society services are offered directly to a child living in Sweden, the child's personal data may be processed on the basis of the child's own consent if the child is at least 13 years old. If the child is under 13, the data may only be processed with the consent of the child's parent or legal guardian.

Health Data Processing in Sweden

In Sweden's healthcare sector, health data can be processed under Article 9 (2)(h) GDPR subject to professional secrecy. Criminal-offence data requires "absolutely necessary" processing and can be processed by private providers under strict necessity.

1.4 Processing of Personal Data for Research and Development Purposes

The GDPR allows further processing for scientific research/statistics/archiving with appropriate safeguards. The Patient Data Act enables use of quality registers for research and statistics.

Healthcare providers may process patient data for quality assurance, healthcare development, and research within healthcare. Processing for commercial product development by external companies requires either patient consent or ethical review board approval combined with appropriate safeguards.

Companies providing healthcare products or services may anonymise patient data for product development and scientific research under specific conditions, as true anonymisation removes data from the GDPR's scope.

European Health Data Space Regulation Impact

The aim of the EHDS Regulation is:

- to improve access to and control over electronic health data for individuals to enable health data to be shared within and between EU countries so that it is available to healthcare professionals and pharmacies when needed for the best possible care and treatment of patients; and
- to enable health data to be reused throughout the EU for purposes such as research, innovation and preparedness for and response to health threats.

For secondary use, the EHDS creates Health Data Access Bodies in each member state to facilitate access to electronic health data for research and innovation. The regulation aims to enable life sciences companies to apply for access to pseudonymised health data across EU member states through standardised procedures.

This is done partly by specifying specific exemptions in Article 9 GDPR to which healthcare data covered by the regulation can apply. It aims to add specific rules for healthcare data to complement the existing rule set in the GDPR.

Aside from this regulation, there have been no national (Swedish) guidelines put in place, or any other laws that regulate the health data space.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Providers and deployers must comply with the GDPR where personal data is processed. Controllers must establish lawful bases for data collection and processing.

There are so far (February 2026) no national guidelines or national AI Act in Sweden. The rules governing AI and automated decisions all stem from the AI Act and the GDPR.

The AI Act regime is risk-based, with prohibited AI uses including manipulative techniques causing significant harm, social scoring, and real-time remote biometric identification for law enforcement (except in narrow cases), as well as certain emotion recognition and biometric categorisation systems.

High-risk AI includes classification for specific areas including biometrics, critical infrastructure, education, employment, essential services (credit/insurance), law enforcement, migration/asylum, justice, and democratic processes.

Transparency and accountability serve as foundational principles across both regulatory frameworks. Within the GDPR framework, organisations must fulfil specific information duties when collecting personal data (for example Article 13 GDPR). The AI Act similarly prioritises transparency, though it implements this principle differently. High-risk AI system providers bear responsibility for equipping deployers with comprehensive usage documentation, enabling them to properly understand and apply the system's outputs (Article 13 AI Act).

Under the EU AI Act (Article 14), "human oversight" refers to the requirement that high-risk AI systems must be designed and developed in such a way that they can be effectively overseen by natural persons during the period in which they are in use, with the aim of preventing or minimising risks to health, safety, or fundamental rights. In practice, this means that persons assigned to oversight must be able to understand the system's capabilities and limitations, detect anomalies, avoid over-reliance on AI outputs (automation bias), correctly interpret results, and crucially, be able to override, disregard, or shut down the system entirely.

In Sweden, IMY has published a guideline which aims to create conditions for combining the development and use of AI with strong data protection, thereby promoting innovation and digitalisation in a privacy-friendly manner.

The guidance stipulates that any processing of personal data in the context of AI development or use must comply with GDPR.

It clarifies what counts as personal data, which includes social security numbers, names, IP addresses, email addresses, and pictures where a person is visible. It also notes that data which cannot on its own be directly linked to a person, but when combined with other data can identify a person, is also personal data.

1.6 Data Breach Requirement

Under the GDPR, controllers must notify IMY within 72 hours unless risk for data subjects is unlikely and inform data subjects without undue delay if high risk is at hand, unless protective measures (eg, encryption) render risk unlikely. Processors must notify controllers without undue delay. Documentation is required.

IMY has their own form, available on their website, which the controllers or processors may fill in to notify a personal data breach. The information required in the form includes:

- incident details: when the incident occurred, when it was discovered, whether it is ongoing, when it ceased, reason for late reporting (if applicable), type of incident (unauthorised disclosure, access, loss, destruction, or alteration), and a brief description;
- discovery and cause: how the incident was discovered and why it occurred, sector and operational area where it took place;
- affected persons and data: number of affected data subjects, number of affected data records, categories of data subjects (employees, customers, patients, children, etc), types of personal data affected (special categories, identification data, etc), and whether data was encrypted;
- consequences: potential consequences of the incident and severity assessment; and
- actions taken: measures taken or planned to address the incident.

Typically, IMY does not investigate a notified breach, as too many are notified to IMY.

Investigations can occur if the breach is receiving a lot of media attention, and IMY feels forced to investigate; see IMY's recent decision issued on 26 January 2026 regarding SportAdmin.

1.7 Regulators IMY

IMY is Sweden's primary data protection regulator. Established under the Data Protection Act, IMY supervises GDPR compliance, the Data Protection Act, and certain sectoral privacy laws. IMY's mandate includes monitoring and enforcing compliance; investigating complaints; conducting audits; issuing guidance; co-operating with other EU supervisory authorities; and representing Sweden in the European Data Protection Board.

Competent Authorities

IMY has authority over all privacy-related matters, except for matters strictly relating to the placement of cookies according to the E-privacy Directive (2002/58/EC). The Swedish Data Protection Authority still has competence to investigate data processing from personal data gathered by cookies.

Investigative Workflow

IMY investigations are typically triggered by:

- individual complaints;
- data breach notifications;
- media reports;
- whistle-blower information; or
- IMY's own initiative based on risk assessments.

Upon receiving complaints, IMY conducts preliminary assessments to determine jurisdiction, admissibility, and priority.

For investigations, IMY typically:

- notifies the controller/processor of the investigation and allegations;
- requests written submissions and documentation;
- provides opportunities for organisations to respond to preliminary findings; and
- issues formal decisions with reasoning, corrective measures, and any sanctions.

Cross-Border Co-Operation

For cross-border processing cases, IMY co-operates with other EU supervisory authorities through the GDPR's consistency mechanism. When IMY is the lead supervisory authority (for controllers/processors

with main establishments in Sweden), it co-ordinates investigations and draft decisions with concerned supervisory authorities. The one-stop shop mechanism aims to provide single-point supervision for cross-border controllers. There are no national rules complementing this structure.

1.8 Enforcement Proceedings and Fines

Investigation Procedure

IMY initiates investigations through various triggers:

- individual complaints (most common);
- data breach notifications suggesting serious violations;
- media reports;
- whistle-blower information; or
- own-initiative investigations based on sectoral risk assessments.

IMY prioritises cases involving: large-scale processing; a special category of personal data; children's data; systematic violations; or novel legal issues with broader implications.

Upon initiating investigations, IMY typically issues written requests for information to controllers/processors, specifying required documentation and response deadlines. The response deadline is typically three weeks, with the possibility of being granted a postponement.

Before issuing decisions, IMY provides draft findings and proposed measures, allowing organisations to submit written responses. This ensures procedural fairness and enables organisations to correct factual errors, provide additional context, or present legal arguments. Unlike, for example, the Swedish Competition Authority, IMY does not have the power to carry out dawn raids, that is, unannounced on-site inspections.

IMY may impose various administrative sanctions under Article 58 GDPR. Warnings and reprimands are non-financial sanctions for less serious violations or first-time offences by organisations demonstrating good faith compliance efforts. Orders to comply with data subject requests address specific rights viola-

tions. Processing suspension orders halt unlawful processing pending compliance.

The most typical sanction is a reprimand, even for more serious breaches. If an administrative fine is issued IMY relies heavily on the Guidelines 04/2022 of the EDPB on the calculation of administrative fines under the GDPR.

Organisations may appeal IMY decisions to Swedish administrative courts. Appeals must be filed with the Administrative Court of Stockholm (*Förvaltningsrätten i Stockholm*) within three weeks of receipt of the decision. Appeals proceed through three levels:

- Administrative Court;
- Administrative Court of Appeal of Stockholm (*Kammarrätten i Stockholm*), requiring leave to appeal; and
- Swedish Supreme Administrative Court (*Högsta förvaltningstribunalen*), requiring leave to appeal.

IMY cannot enforce its actions through criminal or civil courts.

1.9 Enforcement Trends

For the past 24 months IMY has had structural organisational issues internally and seen the amount of incoming complaints increase substantially. As a result, IMY's capacity to carry out own-initiative investigations has dropped significantly. As of 1 January 2026, IMY has introduced a new organisational structure aimed at streamlining the agency to better handle complaints and own-initiative investigations.

Most decisions made by IMY are from complaints lodged against a controller, typically when IMY is the lead supervisory authority according to the one-stop shop mechanism. This is because IMY faces resistance from other supervisory authorities when seeking to close cases without examining the substance of the complaint, for example by issuing information letters instead of adopting a decision on the merits.

In practice, the clearest indication that IMY is likely to commence an own-initiative investigation is that the matter has attracted media attention.

2. Privacy Litigation

2.1 Privacy Litigation Overview

There has been no national case law from the Swedish Supreme Court regarding private litigation. However, there have been several lower court judgments regarding non-contractual damages. Typically, these cases revolve around a data subject's rights not being adhered to.

Most cases are typically not successful in the court because of difficulties proving actual non-contractual damages, even though non-material damages are compensable. The levels of non-contractual damages applicable under Swedish case law are normally between SEK3,000 and SEK5,000 for non-material damages, but in a few isolated cases have been between SEK15,000 and SEK35,000.

The requirements for claimants to bring privacy claims before courts follow the CJEU's case law, which indicates that it is required that there has been an infringement of the Data Protection Regulation, that damage has occurred, and that there is a causal link between the infringement and the damage. An infringement of the provisions of the Data Protection Regulation alone is thus not sufficient to give rise to compensation.

2.2 Recent Case Law

There is no national case law – ie, from the Swedish Supreme Court, regarding privacy litigation; all relevant rules or standards are CJEU case law. The most relevant decisions are:

- judgment of the Court of Justice of the European Union of 4 May 2023 in Case C-300/21;
- judgment of the Court of Justice of the European Union of 14 December 2023 in Case C-340/21; and
- judgment of the Court of Justice of the European Union of 25 January 2024 in Case C-687/21.

Collectively, these three decisions establish the threshold for GDPR compensation claims: a breach alone is not enough; actual (even non-material) harm must be proven, hypothetical fears are insufficient on their own (though genuine, well-founded fear can qualify), and no punitive damages are available.

2.3 Collective Redress Mechanisms

The Swedish legislature has not implemented Article 80 GDPR, which gives organisations or associations in the field of the protection of data subjects' rights and freedom the right to exercise the rights referred to in Articles 77, 78 and 79 of the GDPR.

Under current Swedish law, a legal person cannot represent an individual in court. A non-profit organisation thus cannot act as a representative for the data subject in an administrative case or in a non-contractual damages case in a general court. The provisions on legal representatives in Chapter 12 of the Code of Judicial Procedure are based on the premise that the representative is a natural person.

With regard to the protection of personal privacy, in recent years it has become more common to have non-profit organisations active in the data-protection field. In Sweden, however, this type of activity is still limited.

The Representative Actions Directive was implemented in Sweden on 1 January 2024 through the Act (2023:730) on Group Actions for the Protection of Consumers' Collective Interests. The reform expands the possibilities for bringing representative actions on behalf of consumers, but is not expected to lead to any dramatic increase in the number of cases. The Swedish Consumer Agency has been designated as a qualified entity in Sweden.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

The EU Data Act (Regulation (EU) 2023/2854) has direct applicability from 12 September 2025 in Sweden as in the other EU member states. Supplementary national legislation will, in accordance with the requirements, be enacted in Sweden. The EU Data Act applies to manufacturers, users, data holders, data recipients, third parties, public bodies, cloud service providers, and participants in data spaces involving connected products and associated services.

The regulation covers both personal and non-personal data, governing cross-sector data access and sharing frameworks in relation to the internet of things, cloud computing, and other data processing services. Sweden will, in accordance with the requirements, enact a new Supplementary Act and Ordinance to complement the EU Data Act, specifying definitions, enforcement mechanisms, and sanctions.

Public authorities may request data in exceptional situations, such as public emergencies, but criminal enforcement agencies and tax authorities are excluded from this chapter.

There is no Swedish national law regulating non-personal data except for the EU Data Act.

3.2 Interaction of Data Regulation and Data Protection

The EU Data Act explicitly respects and complements the GDPR and other privacy laws, requiring that data sharing and processing of personal data comply with the GDPR's principles and legal bases. Pseudonymisation or anonymisation of personal data is mandated where feasible for public requests.

Confidentiality obligations apply to competent authorities and public bodies processing data under the EU Data Act, with existing Swedish secrecy laws deemed adequate for covering these requirements.

The EU Data Act prescribes a limitation in the scope of application of the Database Directive. It is thus intended to cover databases even when data is obtained from or generated by a connected product or a related service covered by the EU Data Act, provided that the conditions for the right *sui generis* are met.

The framework ensures that any processing of personal data under the EU Data Act maintains a lawful basis under the GDPR, such as necessity for public tasks or legal obligations, whilst respecting confidentiality and data protection principles.

3.3 Rights and Obligations Under Applicable Data Regulation

Rights

Users of connected products have enhanced rights to access and share product-generated data, with data holders obligated to provide such access promptly and under non-discriminatory, fair terms; unfair contractual clauses are invalidated.

Natural persons and legal entities whose rights under the EU Data Act are infringed have the right to lodge complaints and seek effective remedies, including appeal rights against authorities' decisions not to act on complaints.

Obligations

- Data sharing between businesses, including cloud service providers, must avoid "lock-in" via the removal of switching fees by 2027, enable data portability, and foster interoperability through open standards developed at the EU level.
- Connected products must be designed so that product data is directly accessible to users by default in an easy, secure, free, and machine-readable format. Before sale or lease, sellers/lessors must provide clear information about data types, volumes, storage, and how users can access or delete data.
- Data holders must make readily available data accessible to users without undue delay, free of charge, in a structured and machine-readable format. When users request data sharing with third parties, data holders must provide the data to those third parties under the same conditions. Data holders must not make it unreasonably difficult for users to exercise their rights through manipulative interface design. Where trade secrets are involved, data holders must identify such data and agree on appropriate confidentiality measures.
- Third parties must process received data only for agreed purposes and delete it when no longer necessary to keep. They must not use data for profiling (unless necessary), share it onwards without agreement, make it available to gatekeepers, or use it to develop competing products.
- A contractual term on data access/use or on liability/remedies in case of breach/termination of data-related obligations that has been unilaterally

imposed on another enterprise is not binding on that enterprise if the term is unfair.

Public entities must handle requested data confidentially and may only use data for the specified public interest; data must be deleted when no longer necessary to keep unless archival law applies.

Action Items for Organisations

Organisations should:

- inventory and categorise cloud agreements (SaaS/PaaS/IaaS), noting that Chapter VI of the EU Data Act already applies from 12 September 2025, even for existing agreements;
- identify B2B agreements with data clauses that are either open-ended or run until 11 January 2034 or later, as these will be subject to Article 13 from 12 September 2027;
- assess other agreements with data components for clauses potentially conflicting with the EU Data Act;
- create a “Data Act addendum” for cloud agreements, prioritising updates to switching and portability clauses, using the European Commission’s non-binding model clauses as a starting point;
- build a “2027 list” of B2B agreements affected by Article 13 from 12 September 2027, planning to remove unfair data clauses and renegotiate or terminate agreements before 2027 if they cannot be adapted;
- monitor PTS guidance as the competent authority in Sweden regarding their forthcoming guidance and supervisory practices concerning the EU Data Act; and
- note that Swedish supplementary legislation enters into force on 1 July 2026, primarily addressing supervision, powers, and sanctions rather than altering the contractual rules in the EU Data Act.

3.4 Regulators and Enforcement

The Swedish Post and Telecom Authority (*Post- och Telestyrelsen*, PTS) is designated as the sole competent authority for enforcement and as the certifying body for dispute resolution organisations. PTS has powers to impose fines, issue warnings, investigate complaints, handle sanctions, and promote data literacy among stakeholders.

The Swedish Civil Contingencies Agency (*Myndigheten för civilt försvar*, MCF) supports public sector bodies requiring data to manage exceptional needs, tasked with guiding and preparing these bodies for effective use of the Data Act provisions.

PTS co-operates with IMY and other sectoral bodies to ensure consistent enforcement and alignment with related legislation. Harmonisation efforts, standards development, and legal clarifications are driven mainly at the EU level via the European Commission and the European Data Innovation Board (EDIB), with PTS participating actively; regulatory sandboxing by PTS is proposed to facilitate practical guidance for industry stakeholders.

Sanctions include administrative fines ranging from SEK5,000 to SEK20 million depending on the nature of the actor and violation.

4. Sectoral Topics

4.1 Use of Cookies

The E-privacy Directive, incorporated in Swedish law through the Electronic Communications Act (*lagen (2022:482) om elektronisk kommunikation*), regulates online tracking technologies such as cookies, SDKs, and other device identifiers.

In Sweden, an opt-in model is applied. Data may be stored in or retrieved from a subscriber’s or user’s terminal equipment only if the user consents to it. However, such storage or access is permitted when necessary for the transmission of an electronic message via an electronic communications network or when necessary for the provision of a service at the express request of the user or subscriber.

Consent must meet GDPR standards: freely given, specific, informed, unambiguous, and easily withdrawable. This means:

- **No Pre-Ticked Boxes:** Users must take affirmative action to consent.
- **No Cookie Walls:** Access to websites cannot be conditioned on consent to non-essential cookies.

- Granular Choices: Users must be able to consent separately to different cookie categories.
- Easy Withdrawal: Consent withdrawal must be as easy as giving consent.
- Clear Information: Cookie notices must clearly explain purposes, data collected, and recipients.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised and targeted advertising in Sweden is primarily regulated by the Marketing Act (2008:486), the GDPR, the Electronic Communications Act (2022:482), and – for large platforms – the EU Digital Services Act (DSA). IMY supervises data protection compliance, whilst PTS oversees cookie compliance.

The GDPR requires a lawful basis for profiling and direct marketing and grants an unconditional right to object to direct marketing. The use of automated decisions is restricted. A special category of personal data use in marketing generally requires explicit consent. Children's online consent threshold applies to Information Society Services, which, according to Article 8 GDPR and Chapter 2 Section 4 of the Swedish Data Protection Act, is set at age 13.

Personalised advertising and online marketing require:

- consent – for electronic marketing (email, SMS) to individuals who have not previously purchased similar products/services; and
- legitimate interests – for direct marketing to existing customers, subject to a balancing test and easy opt-out.

Data subjects have an absolute right to object to direct marketing at any time. Controllers must:

- inform data subjects of the right to object at first communication; and
- provide easy, free opt-out mechanisms (eg, unsubscribe links).

Case Law

IMY found that Bonnier News AB processed personal data without legal grounds under Article 6.1 GDPR by profiling individuals based on their behavioural data in complex behavioural profiles and simple behavioural

profiles to display customised advertisements, and imposed an administrative fine of SEK13 million.

IMY found that the consent requirement under Swedish Electronic Communications Act provides strong privacy protection and control for individuals, that this protection risks being undermined if collected personal data is processed based on other legal grounds such as legitimate interest, and that the scope for using Article 6.1 (f) GDPR as a legal basis for profiling based on observed data is limited.

4.3 Employment Privacy Law

Swedish employment law balances employers' legitimate interests in managing the workplace against employees' privacy rights. Key principles include:

- Necessity and Proportionality: Employee monitoring must be necessary for legitimate purposes and proportionate to those purposes.
- Transparency: Employees must be clearly informed about monitoring scope, purposes, and methods.
- Minimisation: Only data necessary for specified purposes can be collected.
- Limited Retention: Employee data can only be retained as long as necessary for the purpose it was originally processed.

It is not advisable to base the processing of employees' personal data on the legal basis of consent. This must only be used in specific situations.

Employee Monitoring

Workplace monitoring (eg, email monitoring, internet usage tracking, location tracking, video surveillance) requires:

- legitimate purpose: clearly defined business reasons (eg, security, productivity, legal compliance);
- proportionality assessment: balancing employer interests against employee privacy;
- transparency: clear policies informing employees about monitoring;
- minimisation: limiting monitoring to what is necessary; and
- good practice in the labour market: an established principle in Swedish labour law, which means that employers and employees must act with respect,

loyalty and common sense, often as a complement to other requirements.

Swedish practice generally prohibits:

- continuous, comprehensive monitoring of all employee activities;
- monitoring of private communications (eg, personal emails, private phone calls);
- covert monitoring except in exceptional circumstances (eg, suspected serious misconduct); and
- monitoring in private areas (eg, restrooms, changing rooms).

Background Checks

There is no express statutory right for informal register checks, though the absence of regulation has not been considered to mean that conducting such checks is prohibited.

For private actors, the problem is that the only applicable legal basis under Article 6 GDPR is often the balancing of interests (Article 6.1 f), which is complicated and creates significant uncertainty for private organisations regarding their right to process such data. Unlike public authorities, private actors lack the right to process data on criminal offences without permission from IMY, except in limited cases where specific statutory support exists.

A fragmented regulatory framework and significant uncertainty about what is permitted mean that currently background checks, especially regarding criminal records, are legally dubious.

A special investigator has been appointed to analyse the need for and prerequisites for conducting background checks in both public and private operations, aiming to provide organisations with appropriate tools before and during employment to prevent risks posed by persons with criminal or other harmful intentions in workplaces, such as infiltration and other undue influence, whilst ensuring personal privacy is protected. The mandate must be completed by 11 March 2027.

Job Applicants

Processing applicant data requires:

- lawful basis: typically, contractual necessity (pre-contractual measures) or legitimate interest;
- transparency: clear privacy notices explaining personal data use;
- retention limits: delete unsuccessful applicant data after two and a half years (to make sure that the time within which an applicant may initiate legal proceedings concerning claimed discrimination related to, for example, age, has elapsed – the time limit is a little more than two years), unless consent has been obtained for future opportunities; and
- equality: avoid discriminatory processing (eg, automated screening tools must not discriminate).

4.4 Data Protection in M&A

There is no specific regulation that differentiates Swedish privacy concerns from any other country bound by the GDPR.

Privacy due diligence is critical to identify risks before acquisition. Key red flags include, for example, lack of privacy policies, no personal data inventory, security issues, and past unresolved data breaches.

Personal data should be disclosed gradually on a “need-to-know” basis throughout the transaction stages. A data sharing agreement between target and acquirer is essential, specifying permitted use, confidentiality obligations, and data deletion requirements if the transaction fails.

Under the GDPR, data subjects must be transparently informed about the M&A transaction and how their personal data will be processed post-completion. The target typically leads this communication through direct contact, website notices, or email notifications. Depending on circumstances, consent may be required for data transfers.

5. International Considerations

5.1 Restrictions on International Data Transfers

Sweden regulates cross-border transfers of both personal and non-personal data through the GDPR and the EU Data Act (Regulation (EU) 2023/2854), sup-

plemented by proposed Swedish national legislation effective from 1 July 2026.

What Counts as a “Transfer”

Under the EU Data Act, “transfer” includes making data available or accessible across member state boundaries or to third countries, encompassing both personal and non-personal data generated by connected products and services. For personal data under the GDPR, transfers occur when personal data is transferred to or accessed from outside the EU or EEA by controllers or processors established within the EU.

Mechanisms for Lawful Transfers of Personal Data (GDPR)

Transfer of personal data to third countries is lawful only if the controller or processor ensures adequate protection via an adequacy decision by the European Commission recognising the third country’s protection level as equivalent to EU standards, or through appropriate safeguards such as binding corporate rules, standard contractual clauses, approved codes of conduct, or certification mechanisms. In the absence of adequacy decisions or safeguards, specific derogations apply for situations, including explicit consent, contract performance, important public interest, legal claims, or protection of vital interests.

Mechanisms for Lawful Transfers of Non-Personal Data (EU Data Act)

Providers of data processing services must implement technical, organisational, and contractual safeguards to prevent unauthorised international government access to non-personal data held in the Union, and transfers pursuant to third-country court orders are only permissible if based on international agreements and provided they meet conditions of specificity, proportionality, and opportunity for objections. Data processing service providers must comply with harmonised rules facilitating data portability and switching of services with technical and contractual safeguards, with fees for switching abolished by 12 January 2027.

The Swedish Post and Telecom Authority (PTS), designated as the competent authority, assesses data requests by public bodies for exceptional needs, ensuring requests meet criteria of necessity, propor-

tionality, transparency, and legitimate interest balance prior to authorising data access. Providers may seek advisory opinions from relevant national bodies on whether conditions for third-country transfers are fulfilled.

Public bodies receiving data via extraordinary needs requests may share data with other public bodies, EU institutions, or approved third parties under conditions preserving confidentiality and purpose limitations. Users have the right to have data held by data holders provided to third parties of their choice on request, subject to contractual safeguards and confidentiality protections, with restrictions on certain entities such as gatekeeper companies. Third parties receiving data must process data only for agreed purposes, maintain confidentiality, and delete data when no longer needed.

Data holders may limit or refuse access to protect trade secrets, confidential business information, or where sharing would significantly harm economic interests, provided they notify PTS. Requests for data by public bodies must be specific, justified, and not duplicate previous requests; unfounded requests need not be complied with.

5.2 Government Notifications and Approvals

Under Article 32 of the EU Data Act, data processing service providers must take adequate technical, organisational, and legal measures to prevent international government access to and transfer of non-personal data held in the Union where such transfer or access would contravene Union law or the national law of the member state concerned. This applies when decisions or judgments from courts or administrative authorities in third countries require a provider to transfer or provide access to non-personal data covered by the EU Data Act and held in the Union.

The decision’s or judgment’s addressee may request an opinion from the relevant national body or authority with competence for international co-operation in legal matters to determine whether the conditions specified are fulfilled, particularly when the decision may concern trade secrets and other commercially sensitive data, as well as content protected by intel-

lectual property rights, or where the transfer may lead to re-identification.

However, Sweden has not succeeded in identifying any authority or body that currently conducts activities corresponding to the task described in Article 32.3 of the EU Data Act. If it emerges during the application of the regulation that data processing service providers do not receive the assistance prescribed in Article 32.3 by approaching Swedish authorities, the government will consider appointing one or more relevant authorities under that article.

5.3 Data Localisation Requirements

Data Localisation Rules

The key Swedish data localisation law is the Swedish Bookkeeping Act (1999: 1078) (*Bokföringslagen*). Chapter 7, Section 2 requires organisations to:

- store accounting information in Sweden for seven years after the end of the calendar fiscal year; and
- maintain equipment for storing accounting information in Sweden.

The types of information that have to be kept in Sweden include:

- balance sheets;
- basic accounting and general ledgers;
- subsidiary ledgers;
- verification documents, meaning documents concerning business events or adjustments made to accounts (Chapter 1, section 2 (8), Bookkeeping Act);
- bookkeeping system documentation and processing histories; and
- annual reports.

Exemptions

An organisation that has accounting obligations under the Bookkeeping Act may:

- temporarily store verification documents outside of Sweden if special reasons consistent with good accounting practices exist (Chapter 7, Section 3, Bookkeeping Act); for example, a bank may store verification documents in another country for bookkeeping in that country;

- store machine-readable media and maintain equipment for storing accounting information in another EU country or a country that is party to a mutual assistance agreement if the organisation:

- (a) notifies the Tax Agency or the Financial Supervisory Authority of the equipment storage location;
- (b) allows immediate access to the accounting information at the request of the Tax Agency or the Customs Agency; and
- (c) can immediately produce the accounting information in printed form on request.

In General

The GDPR does not mandate data localisation; personal data may be stored anywhere provided appropriate transfer mechanisms are in place. However, remote access by third-country entities constitutes a transfer requiring compliance with Chapter V GDPR.

Remote access by third-country entities is permitted when:

- the third country has received an EU adequacy decision (eg, EU-US Data Privacy Framework for certified US organisations, UK, Switzerland, Japan, etc); and
- standard contractual clauses (SCCs) have been executed between data exporter and importer, accompanied by:
 - (a) transfer impact assessment evaluating third-country laws;
 - (b) supplementary measures where necessary (encryption, access controls, data minimisation); and
 - (c) documentation of assessment and measures;
- for intra-group transfers, binding corporate rules (BCRs) have been approved by supervisory authorities;
- Article 49 derogations apply in limited situations, including:
 - (a) explicit consent after being informed of risks;
 - (b) contractual necessity;
 - (c) legal claims establishment, exercise or defence;
 - (d) vital interests protection; and
 - (e) compelling legitimate interests (rare, occasional transfers affecting few individuals);

- irrespective of the transfer mechanism relied upon, appropriate technical and organisational security measures have been implemented, namely:
 - (a) encryption of data in transit and at rest;
 - (b) strong authentication and access controls;
 - (c) logging and monitoring of access;
 - (d) contractual restrictions on data use; and
 - (e) regular security assessments.

5.4 Blocking Statutes

There is no privacy law except for the GDPR restricting foreign discovery. The basic principle is that a court in the state where the trial is taking place can only access evidence in another state if that state has given its consent, either through an international agreement or in the individual case. If an official representative of a state, such as a judge, conducts evidence-gathering on site within the territory of another state without such approval, this typically constitutes a violation of the sovereignty of the other state.

Rules on the taking of evidence abroad are found in the 1970 Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters. Between EU member states, the EU Evidence Regulation (Regulation (EU) 2020/1783) applies. If there are legal grounds for foreign discovery, these would typically not be in conflict with the GDPR, as the regulation permits processing of personal data for secondary purposes if it is based on Union law or the national law of the member states, and constitutes a necessary and proportionate measure in a democratic society.

The Swedish Supreme Court addressed the interplay between discovery obligations and the GDPR in the *Norra Stockholm Bygg* case (Ö 1750-20), where it sought a preliminary ruling from the CJEU on whether GDPR Articles 6 (3) and 6 (4) apply to national procedural law concerning discovery of documents containing personal data. The CJEU confirmed that these provisions are applicable in civil disputes involving discovery of documents with personal data concerning third parties collected for other purposes (such as tax control). The court held that national courts must consider the interests of the data subjects when deciding on discovery requests and balance these against the circumstances of each case, the type of proceedings involved, and with due regard to the proportionality principle and the data minimisation principle under Article 5 (1)(c) GDPR.

In the Swedish case, the Swedish Supreme Court ultimately granted the discovery request, emphasising that the right to effective judicial protection and a fair trial requires parties to access documents needed to prove their case, even when they contain others' personal data. However, it applied the data minimisation principle by requiring masking of personal identity numbers whilst allowing disclosure of names and work attendance records.

5.5 Recent Developments

The GDPR continues to evolve through adequacy decisions and updated SCCs. The AI Act's entry into force (general application from 2 August 2026; prohibitions from 2 February 2025) will add obligations for high-risk AI relying on cross-border data and require alignment with GDPR and data-transfer regimes. The changes to be expected next is the matter of the EU-US Data Privacy Framework and whether it will be challenged in the courts.

Trends and Developments

Contributed by:

Niclas Rockborn, Astrid Svensson and Ivan Sivik
Gernandt & Danielsson

Gernandt & Danielsson offers bespoke advice on data protection regulation, including considerations involving other areas of regulatory compliance, such as artificial intelligence and the financial regulatory landscape, in order to ensure a holistic approach. The firm acts for domestic and international clients

on data protection issues, compliance work and data breaches. It is very strong on large transactional matters and the team provides transactional data protection advice, including data protection due diligence and audits.

Authors



Niclas Rockborn heads Gernandt & Danielsson's specialist practice group. He has more than 25 years' experience advising clients who offer financial services, including entities in banking and insurance, asset

management, e-money and payment institutions, and various operators in the fintech sector. Niclas also has extensive experience advising investors in alternative investment funds and in connection with the establishment of alternative investment funds.



Ivan Sivik is an associate at Gernandt & Danielsson and works in the firm's specialist practice group. He has a special focus on financial services.



Astrid Svensson is a senior associate at Gernandt & Danielsson and has a primary focus on data protection, which she has focused on since the implementation of the GDPR. She is well versed in, and assists with,

complex data privacy and data protection issues, such as assessments of legitimate interests, data protection impact assessments, privacy by design and transfers of personal data to third countries. Astrid also has extensive experience in advising on data protection matters in transactions. In addition, her practice covers IT law, artificial intelligence law, commercial agreements and intellectual property rights. Astrid is a member of the Swedish Bar Association.

Gernandt & Danielsson

Hamngatan 2
Box 5747
SE-114 87
Stockholm
Sweden

Tel: +46 8 670 66 00
Email: info@gda.se
Web: www.gda.se



General Trends

In recent years, Sweden's approach to data protection has significantly evolved. Rapid technological advancements, increased digitalisation across industries, and a growing awareness of individuals' right to privacy are the main drivers of this development. As a member of the European Union (EU), the Swedish data protection regime mainly consists of the General Data Protection Regulation (GDPR) and national laws supplementing the GDPR.

This update highlights three prominent data protection trends in Sweden. The first trend concerns cybersecurity and digital resilience in the financial sector from a data protection perspective. The second trend addresses technological advancements and the interplay between artificial intelligence (AI) and data protection. The third trend regards Swedish developments concerning the processing of personal data relating to criminal convictions and offences.

Trends in the Financial Sector From a Data Protection Perspective

The Swedish financial sector in general

The Swedish financial sector is highly digitalised and includes traditional banks and, to a large extent, fintech leaders such as Trustly, Klarna and Zettle. This digitalisation entails data protection as well as information and communication technology (ICT) risks, rendering the Swedish financial system particularly vulnerable to data protection risks, cyber threats, and ICT disruptions. In addition to recent developments in EU data and cyber regulations, several of which have already entered into force and are expected to be implemented in 2026, the heightened focus on cybersecurity also responds to changes in the Swedish security landscape arising from, inter alia, the ongoing war in Ukraine and organised crime.

Swedish banking secrecy

The Swedish banking secrecy rules apply in parallel to the GDPR. Hence, data may fall under the scope of both the GDPR and Swedish banking secrecy rules, requiring careful assessments to ensure compliance with both sets of rules. Swedish bank secrecy is regulated in the Swedish Banking and Financing Business Act (*Lag (2004:297) om bank- och finansieringsrörelse*) but also in other laws applicable to specific sectors

within the financial industry. The Banking and Financing Business Act provides that a credit institution may not disclose an individual's relationship to the credit institution without authorisation. This duty of secrecy imposes obligations on the credit institution and its representatives, such as employees, the CEO, and contractors. If a bank violates banking secrecy undertakings, it could be liable for damages if the individual can prove that the relevant breach has caused them financial harm. Such violations may also prompt the Swedish Financial Supervisory Authority (SFSA) (*Finansinspektionen*) to review the bank's general procedures, potentially resulting in sanctions if the SFSA deems these procedures inadequate.

The individuals to whom the right to confidentiality applies are the bank's natural and legal customers. It applies to all current and former customer relations, regardless of the duration and extent of the relationship, and extends beyond the death of the natural person or the dissolution of the legal entity. The protected information is interpreted broadly to include all information about the customer that the bank obtains because of the customer relationship, both personal data and trivial private information, even if it is not obtained directly from the customer.

Exceptions to banking secrecy apply when providing information to legal guardians, during criminal investigations, and in other instances, provided that there are legitimate grounds. Banking secrecy may also be waived by a provision of law or based on other specific legitimate grounds (not to be confused with "legitimate interest" under the GDPR). Banking secrecy does not apply to the customer themselves or when the customer has consented to a specific information disclosure. Additionally, information that is already publicly known is not considered confidential and is therefore not protected by banking secrecy regulations.

As part of the government's ambitions to fight criminal activities, since April 2025, banks and payment institutions have been subject to obligations to disclose customer information to law enforcement authorities pursuant to the Swedish Banking and Financing Business Act (*Lag (2004:297) om bank- och finansieringsrörelse*) and the Swedish Act on Payment Services

(*Lag (2010:751) om betaltjänster*). The disclosure obligation overrides the duty of confidentiality and provides a legal basis for the processing of personal data relating to criminal offences. The government has also introduced the same disclosure obligation for e-identification companies and crypto service providers, proposed to enter into force in May 2026.

The EU Digital Operational Resilience Act

The EU Digital Operational Resilience Act (DORA) (Regulation 2022/2554) establishes requirements to address ICT-related risks for most financial undertakings operating in Sweden. DORA aims to mitigate ICT vulnerabilities and establish uniform rules across the EU. It introduces, inter alia, requirements for cybersecurity information, continuity planning, managing risks from outsourcing ICT to third parties, resilience testing, and frameworks for information sharing.

Effective from January 2025, DORA and supplemented technical standards apply to banks, investment firms, insurance companies, and other financial undertakings, such as managers of alternative investment funds and crypto service providers. As the financial sector has become predominantly digital and reliant on third-party infrastructure and service providers, such ICT providers fall within the scope of DORA. The Swedish Act (*Lag (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn*), supplementing DORA and regulations from the SFSA, set out provisions on threat-led penetration testing, fees, sanctions, and supervision by the SFSA.

Additionally, DORA poses certain data protection requirements that must be fulfilled. Financial entities must assess ICT risks and discontinuation provisions to ensure appropriate data protection prior to entering into a contractual arrangement on the use of ICT services. This includes provisions on availability, authenticity, integrity, and confidentiality in relation to the protection of data, including personal data.

The EU NIS 2 Directive

The NIS 2 Directive (NIS 2), adopted by the EU in December 2022, aims to achieve a higher level of cybersecurity within the EU by significantly expanding the scope of covered sectors, enhancing require-

ments for security measures and incident reporting, strengthening management responsibilities, and introducing stricter sanctions. NIS 2 was implemented into Swedish law through a new Cybersecurity Act (*Cybersäkerhetslag (2025:1506)*) that entered into force in January 2026. It should be noted that financial institutions shall for certain provisions adhere to the DORA as *lex specialis*.

In addition, the Critical Entities Resilience Directive (CER) (CER Directive 2022/2557), adopted by the EU in December 2022, aims to strengthen the resilience of critical entities against disruptions to their operations. With few exceptions, NIS 2 and CER cover entities operating in the same sectors, such as the energy and transport sectors. However, entities in the banking, financial market infrastructure, and digital infrastructure sectors are to some extent exempt from certain provisions of the new law transposing CER into Swedish law as similar obligations are already covered by NIS 2 and the Cybersecurity Act. The final legislative proposal for the implementation of CER into Swedish law is preliminary scheduled for publication in March 2026, and is preliminary set to enter into force during spring/summer 2026.

It should be noted that the Commission proposed the Digital Omnibus Package in November 2025, which aims to provide a solution for streamlining cybersecurity incident reporting under several laws, including the GDPR, NIS 2 and CER, bringing them under the umbrella of a single reporting mechanism for all related reporting obligations.

The new Consumer Credit Directive

To strengthen consumer protection, the EU has adopted a new Consumer Credit Directive (CCD 2). The directive is expected to be implemented into Swedish law through a proposed new Consumer Credit Act (*Konsumentkreditlag*), with a government bill anticipated in March 2026 (although currently delayed) with entry into force in November 2026. CCD 2 affects data protection in several ways.

Firstly, the Swedish government proposes to introduce an obligation for creditors and credit intermediaries to inform consumers in a clear manner that they are providing them with a personalised offer based on

the automated processing of their personal data, and to inform them of the data sources used to personalise such offers.

Secondly, similar to Article 22 of the GDPR, the CCD 2 grants consumers the right to request and obtain human intervention from the creditor where an automated credit assessment decision is based on personal data. Additionally, the CCD 2 provides individuals with a broader right to human intervention as it applies to the entire credit assessment process and not just to the final decision.

Thirdly, the CCD 2 prohibits the collection and processing of sensitive personal data contained in databases for the purpose of assessing the consumer's creditworthiness.

Finally, the CCD 2 stipulates that consumers must be informed within 30 days of registration in a database of any outstanding credit claims about the registration itself and about their rights under the GDPR. As no corresponding right to information exists in Swedish law, the government intends to introduce such a provision.

AI and Data Protection

The AI Act and data protection

The AI Act came into effect in August 2024, and its provisions are being implemented gradually. It aims to promote the use of human-centred and trustworthy AI, and to protect users against harmful effects. The AI Act governs the development, provision, and use of AI systems in the EU. It employs a risk-based approach, where AI systems are divided into the following categories of risk:

- unacceptable;
- high;
- limited; and
- minimal.

Different requirements apply based on the risk category. General-purpose AI models are an additional category posing specific transparency requirements.

The AI Act applies in parallel with the GDPR. A national review of the need for national adaptations because of

the AI Act has been published and the supplementary provisions are proposed to enter into force in August 2026. With regard to market surveillance, the government has proposed that supervisory responsibilities will be delegated to different authorities, each responsible for supervising AI systems in their respective areas. Additionally, the Swedish Authority for Privacy Protection (IMY) (*Integritetsskyddsmyndigheten*) will be responsible for the supervision of several high-risk AI systems and prohibited AI uses. The Swedish Post and Telecom Authority (PTS) (*Post- och telestyrelsen*), as the single contact point, will be responsible for coordinating market surveillance, supervision, and for leading activities in AI regulatory sandboxes. Finally, IMY, PTS and SFSA are also tasked with authorising real-world testing outside regulatory sandboxes.

IMY's regulatory sandboxes

The use and integration of AI in various sectors raise significant concerns from a data protection perspective, which need to be evaluated on a case-by-case basis. One of the foremost challenges is understanding the impact of the GDPR on AI and vice versa. IMY has been actively involved in addressing the emerging challenges of new AI technology through regulatory sandboxes. Uncertainty generally stifles innovation; therefore, IMY offers guidance through its regulatory sandboxes, which emphasise the use of AI in relation to data protection regulations.

Throughout 2025, IMY launched and concluded several sandbox projects. One notable regulatory sandbox project concluded in 2025 focused on data protection issues arising from the further processing of personal data for the purpose of training AI models. The project examined whether further processing of actual personal data and synthetically generated data for AI model training would be compatible with the purpose limitation principle under the GDPR.

IMY concluded that the training of AI models with personal data or with synthetically generated data cannot be considered to be for statistical purposes. IMY further assessed that neither the training of AI models with personal data nor with synthetically generated data can be considered to be further processing that is compatible with the original purposes. However, IMY considered that further processing could be per-

missible if additional safeguards in the form of opt-out solutions are provided when information is given to data subjects, and that the synthesis of personal data for training AI models is a privacy-friendly way of reducing risks to the infringement of privacy rights.

Another interesting sandbox concluded in 2025 concerned the “Sharing of customer data between banks to counter financial crime”. Through the regulatory sandbox, IMY collaborated with the four major Swedish banks – SEB, Nordea, Swedbank and Handelsbanken – to explore the legal possibility of flagging high-risk individuals in a shared system to prevent financial crimes. The project concluded that this type of information sharing constitutes processing of criminal data under Article 10 of the GDPR and that there is probably no legal basis for banks to carry out such processing. That is in part because IMY assessed that in light of banking secrecy provisions in the Swedish banking secrecy and confidentiality provisions in the Money Laundering Act and Terrorist Financing (Prevention) Act (*Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism*) and the Payment Services Act (*Lag (2010:751) om betaltjänster*), it would be difficult for banks to base the intended sharing of personal data on legal violations on the legal basis of legitimate interest.

A noteworthy regulatory sandbox to monitor in 2026 is IMY’s regulatory sandbox project with a municipality to explore the safe and responsible use of AI in social services. The initiative focuses on testing AI tools for recording, transcribing, and summarising conversations. The objective is to reduce social workers’ administrative burden and free up more time for client contact.

Personal Data Relating to Criminal Convictions and Offences

Article 10 of the GDPR and its interpretation

Article 10 of the GDPR concerns the processing of personal data relating to criminal convictions and offences. In Sweden, the general rule is that only the public authorities can process personal data related to criminal convictions and offences. The legal bases for organisations, other than public authorities, to process personal data of this nature are limited to when permitted under the Swedish constitution, applicable

law, or when necessary to establish legal claims or fulfil legal obligations. In addition, IMY has the authority to permit organisations to process personal data related to criminal offences.

According to IMY, Article 10 of the GDPR shall be interpreted to apply to information that discloses whether a person is or has been the subject of a police report, preliminary investigation, prosecution, or proceedings in criminal cases. This also includes acquittals in criminal cases, for example, if a person has been released from accusation and freed from obligation regarding the charges. IMY’s statement further clarifies that information indicating that a natural person has or may have been suspected of criminal activities can be considered to fall within the scope of Article 10 of the GDPR, regardless of whether legal proceedings have been initiated. This shall not be interpreted to include all information, as there is a certain threshold of specificity to be met.

Additionally, IMY clarifies that observations or passive events where the objective criteria for a crime may be met are normally not considered processing of personal data relating to criminal convictions and offences. Simply put, if a surveillance camera captures a robbery through passive recording of a certain area, this would generally not be considered data processing under Article 10 of the GDPR. On the other hand, if the sequence of events is separated at a later stage for legal action, it will fall under the scope of Article 10 of the GDPR.

Checks against sanction lists

Another development concerns the legality of conducting checks against sanction lists. The processing of personal data concerning criminal convictions and offences was to some extent already permissible under the Swedish Money Laundering and Terrorist Financing (Prevention) Act to the extent necessary to assess and manage the risks associated with a customer relationship. However, there was no explicit legal basis for conducting checks against sanction lists.

Organisations within, for example, the financial, dual-use and military sectors frequently need to perform checks against various international sanction lists

for compliance reasons, such as sanction lists from OFAC, OFSI and the EU. As a consequence, unless other applicable laws authorise checks against sanction lists, for example, through EU regulations, businesses in Sweden have been required to seek specific permission from IMY to be able to conduct checks against sanction lists since sanction lists may contain information about criminal offences. This resulted in IMY receiving an excess of applications from entities within the financial sector seeking permission to process such personal data to comply with anti-money laundering and terrorism financing obligations, as well as from undertakings involved in the export of dual-use goods or military equipment to adhere to international export restrictions.

IMY's updated regulation and related guidelines aim to facilitate the processing of personal data relating to criminal convictions and offences by certain sectors. This will allow certain entities within the financial sector and military industry to process personal data relating to criminal convictions and offences when conducting checks (for example, customers, suppliers, and employees against sanctions lists).

The Swedish entities affected by the new regulations are companies in the financial sector under the supervision of the SFSA, companies in the security and defence market under the supervision of the Swedish Inspectorate for Strategic Products (*Inspektionen för strategiska produkter*), and certain companies in the security and defence market under the supervision of the Swedish Radiation Safety Authority (*Strålsäkerhetsmyndigheten*).

GDPR and the constitutionally protected right to publish

For non-Swedish persons, it may come as a surprise how easily the personal data of most Swedish individuals can be found in online databases, including name, family, address, size of home, car details, company engagements, criminal records, etc. Under the Swedish Freedom of the Press Act (*Tryckfrihetsförordningen* (1949:105)) and the Swedish Fundamental Law on Freedom of Expression (*Yttrandefrihetsgrundlagen* (1991:1469)), holders of a certificate of no legal impediment to publication – ie, a publishing licence,

have constitutional protection for their publication of personal data.

The compatibility of personal data publishing and the GDPR has been the subject of several governmental investigations and national public debate due to the widespread publication of personal data, including personal data relating to criminal convictions and offences. Previously, the general opinion was that IMY was prevented from investigating complaints from individuals against search services because of the protection under the Swedish Freedom of the Press Act and the Swedish Fundamental Law on Freedom of Expression.

However, in 2025, IMY reconsidered its legal position concerning the right of entities with voluntary publishing licences to publish personal data under the Swedish constitution in relation to the GDPR. IMY now considers itself authorised to supervise search services with a publishing licence following complaints from individuals under the GDPR. This reconsideration was prompted by developments in EU and Swedish case law that have strengthened the legal rights of individuals who file complaints and clarified that a balance must be struck in each individual case between data protection rights under the GDPR and the constitutional protections for freedom of expression.

Data relating to criminal convictions and offences may be relevant for background checks but is generally prohibited from being processed by companies unless expressly permitted by law or authorised by IMY. IMY publishes a list of entities granted such authorisation on its website. The Swedish government has appointed an inquiry, scheduled to report its findings on 11 March 2027 at the latest, to assess how background checks involving criminal records in the public and private sectors can be conducted to mitigate security risks while ensuring compliance with data protection regulations.

Following the aforementioned legal developments, IMY has initiated supervision of several companies that hold a publishing licence and provide online search services with sensitive personal information. It will be of interest to observe how this development unfolds during the coming year and the extent to which it may affect these companies' operations and the availability of this category of data.



Law and Practice

Contributed by:

Che-Hung Chen, Doris Lu, Jakob Huang and Meng-Ying Lee
Chen & Lin

Contents

1. Legal and Regulatory Framework p.477

- 1.1 Overview of Data and Privacy-Related Laws p.477
- 1.2 Rights and Obligations p.479
- 1.3 Special Categories of Personal Data p.480
- 1.4 Processing of Personal Data for Research and Development Purposes p.480
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.480
- 1.6 Data Breach Requirement p.481
- 1.7 Regulators p.481
- 1.8 Enforcement Proceedings and Fines p.482
- 1.9 Enforcement Trends p.483

2. Privacy Litigation p.484

- 2.1 Privacy Litigation Overview p.484
- 2.2 Recent Case Law p.484
- 2.3 Collective Redress Mechanisms p.485

3. Requirements for the Protection and Processing of Non-Personal Data p.485

- 3.1 Objectives and Scope of Data Regulation p.485
- 3.2 Interaction of Data Regulation and Data Protection p.486
- 3.3 Rights and Obligations Under Applicable Data Regulation p.486
- 3.4 Regulators and Enforcement p.487

4. Sectoral Topics p.487

- 4.1 Use of Cookies p.487
- 4.2 Personalised Advertising and Other Online Marketing Practices p.487
- 4.3 Employment Privacy Law p.488
- 4.4 Data Protection in M&A p.488

5. International Considerations p.489

- 5.1 Restrictions on International Data Transfers p.489
- 5.2 Government Notifications and Approvals p.489
- 5.3 Data Localisation Requirements p.490
- 5.4 Blocking Statutes p.490
- 5.5 Recent Developments p.490

Chen & Lin counts data protection as one of its main practice areas, due to the emerging technologies that are accumulating, compiling and analysing immense volumes of data. In total, the data protection group has 15 lawyers, who provide advice and assistance to clients from all over the world. The team combines legal experience and adaptability with advanced hi-tech skills and development. The firm is also well connected with law firms in other countries and is able to provide an international service as a result of co-operation and co-ordination with those firms.

Key practice areas include compliance; providing the latest regulatory developments; advising on appropriate measures for protecting an owner's data and not infringing another's right to data; reviewing and commenting on market practice relating to data protection; handling dispute resolution; assisting clients in navigating investigations or court proceedings; defending allegations of infringement; and asserting and enforcing data protection regulations or contract arrangements.

Authors



Che-Hung Chen is the partner in charge at Chen & Lin. His key practice areas relate to intellectual property, funding/capital, and market behaviour and activities. Che-Hung Chen continues to practise in cases relating

to data protection and is currently handling a series of trade secret cases involving the protection of R&D data. Although there are limited professional bodies that relate to the practice of data protection law specifically, he is a frequent participant in activities relating thereto.



Jakob Huang is a partner at Chen & Lin and practises in the areas of M&A, inbound and outbound investment, general corporate consultations, contractual business model design, and the drafting and negotiation of

various contracts. He provides a data protection service to corporate clients in various fields of business, and provides data protection advice to e-commerce, video games and social media companies on their compliance with personal data protection regulation.



Doris Lu is a partner at Chen & Lin and is experienced in the practice areas of overseas and domestic M&A transactions, inbound and outbound investment, IPO/SPO and fundraising, financing, general corporate

consultations, data centre development projects and data protection practice. She frequently provides data protection advice and assists in high-profile data incident investigation and project-type data protection compliance investigations for various clients, most of which are multinational corporate clients, including data centres, luxury brands and other data-rich enterprises, and Taiwan listing companies.



Meng-Ying Lee is an associate at Chen & Lin, whose key practice areas are litigation, corporate consultation and legal compliance. She has advised clients on data protection and privacy laws and has provided

analysis of the resulting impact on data protection considerations from the perspective of Taiwan law for clients' issues. She frequently provides data protection services, including compliance, high-profile data incident investigation and project-type data protection compliance investigation, to various clients, including multinational data centres, luxury brands and other data-rich enterprises.

Chen & Lin Attorneys-at-Law

Bank Tower, 12th Floor
205 Tun Hwa North Road
Taipei 105
Taiwan (Republic of China)

Tel: +886 2 2715 0270
Fax: +886 2 2514 7510
Email: dorislu@chenandlin.com
Web: www.chenandlin.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Data Protection and Privacy Law Sources in Taiwan

The Personal Data Protection Act (PDPA) is the primary law regulating personal data protection. It was first enacted in August 1995, as the Computer-Process Personal Data Act, and regulated government agencies and certain private sectors. The PDPA has been effective since 1 October 2012 and regulates any person – including government agencies and all private sector entities – who collects, processes or uses personal data. Privacy and personal data protection are related to the constitutional protection of privacy.

In addition to the PDPA, the Legislative Yuan has also enacted certain special data protection requirements in some sector-specific laws, such as:

- the Insurance Act;
- the Financial Holding Company Act;
- the Banking Act;
- the Human Biobank Management Act;
- the Pharmaceutical Affairs Act; and
- the National Sports Act.

Furthermore, the Trade Secrets Act may apply if the trade secrets of an enterprise are involved. If an offence against computer security is involved, the criminal sanctions of the Criminal Code of the Republic of China may apply. If any national security issue is involved, the National Security Act may apply.

On 16 May 2023, the Legislative Yuan passed amendments to the PDPA to urge non-government agencies (ie, the private sector) to input manpower, techniques and funds for the purpose of fulfilling data protection obligations, and to provide support to relevant enforcement authorities for combating fraudsters. Two main points of the 2023 amendments are as follows:

- raising the administrative penalties imposed against non-government agencies for violating the obligation of security and maintenance measures; and
- designating the Personal Data Protection Commission (PDPC) as the dedicated competent authority of the PDPA (the Preparatory Office of the PDPC was formed on 5 December 2023, accordingly).

On 11 November 2025, further amendments to the PAPA were promulgated; however, their effective date has not yet been determined. The main purpose of these amendments is to align with the PDPC to be established (which is a Preparatory Office now) and to grant the PDPC relevant enforcement powers, including administrative supervision over both government and non-government agencies, as well as co-operation mechanisms with other competent authorities with regard to supervision on non-government agencies.

The main points of these amendments are as follows:

- the establishment of a supervision mechanism for government agencies;

- the obligation for government agencies and non-government agencies to implement response measures, maintain records of incidents, and report personal data breaches, along with the revision of the conditions for notifying the affected parties; and
- transition of supervisory authority – the amendments establish transitional arrangements for the gradual transfer of supervisory authority over non-governmental agencies' personal data protection matters to the PDPC. During the transition period, designated central or local authorities will continue to exercise supervisory powers, which will be progressively assumed by the PDPC. The relevant competent authorities will continue to administer industry-specific data protection regulations and may prescribe more stringent requirements.

For clarity, unless otherwise referred to, the PDPA referred to herein will be the version amended and passed on 11 November 2025.

The national system in respect of data protection adopts an “APEC-EU referential” approach. The meeting minutes of the Executive Yuan in connection with the approval to submit the draft bill of the PDPA to the Legislative Yuan addressed that the PDPA incorporates certain provisions under Directive 95/46/EC. As one of APEC’s member economies, Taiwan has executed the APEC Privacy Framework, which indicates nine principles in respect of privacy protection; the PDPA also incorporates the principles guided by the APEC Privacy Framework.

In 2011, APEC developed the Cross-Border Privacy Rules (CBPR) system, under which companies trading within the member economies develop their own internal business rules consistent with the APEC privacy principles to secure cross-border data privacy. Taiwan joined the CBPR system in December 2018, with the Institution for Information Industry applying to be the Accountability Agent under the system. In June 2021, the Institute for Information Industry was recognised by APEC as the Accountability Agent for CBPR verification in Taiwan for domestic enterprises.

Taiwan also joined the EU-led Joint Declaration on Privacy and the Protection of Personal Data in October

2022. The declaration is intended to foster international co-operation to promote high data protection and privacy standards. Taiwan’s inclusion will allow strengthening exchanges and co-operation with EU and Indo-Pacific countries.

Furthermore, in seeking an “adequacy decision” from the European Commission, the Personal Data Protection Office has filed the evaluation reports required for GDPR adequacy status; the application is still under review and discussion. All major laws regulating privacy and personal data protection are at the national level. The relevant regulations at the sub-national level are solely relevant to the implementation of those national laws and regulations by the different functioning bureaus of local government. Additionally, certain competent authorities have established specific regulations requiring security and maintenance plans for the protection of personal data within the industries under their supervision. These regulations are applicable to each specific industry.

The PDPA provides for extraterritorial application under defined circumstances. It applies to both government agencies and non-government entities that, outside the territory of Taiwan, collect, process or use the personal data of Taiwanese nationals. Accordingly, the territorial scope of the PDPA is extended based on the nationality of the data subject, irrespective of the location where the data-related activities are conducted.

Furthermore, criminal liability for intentional violations is established by specified provisions of the PDPA, including unlawful collection, processing, use, alteration or deletion of personal data, where such conduct is undertaken for the purpose of obtaining unlawful benefits for oneself or a third party, or of harming the interests of others, and where such conduct results in actual damage. The law expressly provides for extraterritorial criminal jurisdiction by stipulating that when Taiwanese nationals commit the aforementioned offences against other Taiwanese nationals outside the territory of Taiwan, the PDPA shall likewise apply.

In conclusion, the PDPA has extraterritorial effect where personal data relating to Taiwanese nationals is handled abroad, and where Taiwanese nationals

engage in specified misconduct involving personal data against other Taiwanese nationals outside Taiwan, thereby subjecting such conduct to the regulatory and criminal enforcement mechanisms of the PDPA.

Artificial Intelligence Fundamental Act and Interplay Between AI and Data Protection Regulations

Taiwan's government also acknowledges the rapid development of emerging technologies, such as AI, and the complex data-related challenges these innovations bring. As a result, the government is also continuously revisiting and examining whether the current regulatory regime could duly catch all new relevant technologies. Under the AI trend, the Artificial Intelligence Fundamental Act was passed by Taiwan's Legislative Yuan on 23 December 2025, and sets out a framework for the development and deployment of AI, guided by seven key principles: "Sustainable Development and Welfare", "Human Autonomy", "Privacy Protection and Data Governance", "Cybersecurity and Safety", "Transparency and Explainability", "Fairness and Non-discrimination" and "Accountability". These principles are designed to ensure that AI technologies are developed in a responsible and ethical manner, balancing innovation with public trust and societal well-being.

Among these, the principle of Privacy Protection and Data Governance plays a critical role in safeguarding individuals' rights in the face of rapidly advancing AI technologies. The Act specifically mandates that AI development must prioritise the protection of personal data privacy, reflecting a commitment to constitutional privacy rights. This includes a focus on minimising the collection and use of personal data, ensuring that only data which is necessary for AI purposes is gathered. By adopting the data minimisation principle, the law seeks to prevent unnecessary data collection that could increase the risk of privacy breaches or misuse.

The interplay between AI and data protection regulations is critical in ensuring that AI technologies do not infringe on privacy rights or create unintended security risks. As AI relies heavily on large datasets to make predictions and decisions, there are significant concerns about how this data is managed. The Artificial Intelligence Fundamental Act seeks to ensure that AI

systems adhere to stringent data protection principles while also driving innovation.

Following the enactment of the Artificial Intelligence Fundamental Act and the announcement of the core principles thereunder, it is anticipated that the Taiwan authorities will further promulgate implementing regulations and establish a more comprehensive and structured regulatory regime in line with the continued development, deployment and utilisation of artificial intelligence technologies.

1.2 Rights and Obligations

General Principles and Data Subject Rights Under the PDPA

Principles and requirements for personal data processing include the following.

- Lawfulness and purpose limitation – personal data should only be collected, processed and used for specific, legitimate purposes. In principle, data should only be processed within the defined scope and not retained longer than the period initially communicated to the data subject. Any further processing for new purposes requires additional consent or a lawful basis.
- Ensure accuracy of personal data – the accuracy of personal data must be ensured, and it should be corrected or supplemented when necessary, either proactively or upon the request of the data subject.
- Transparency – data subjects should be fully informed about the collection of their data. This includes, among others, detailing who is collecting the data, the purpose behind the collection, what types of data are being gathered and how it will be used. Additionally, data subjects should be made aware of their rights, such as access, correction and deletion of their personal data.
- Security and confidentiality – appropriate security measures must be in place to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.
- Respect for data subject rights – the rights of individuals to access, correct or erase their personal data must be respected and facilitated by organisations. Data subjects should be able to easily exercise their rights in a transparent and user-friendly manner.

- Restrictions on international transfer – when the competent authority imposes restrictions on international data transfers, non-government agencies must comply with these limitations and refrain from transferring the data.

Data subject rights include the following:

- access and inspection of personal data;
- obtain copies of personal data;
- correction or supplementation of personal data;
- suspension of collection, processing or use; and
- deletion of personal data.

A compliance checklist includes the following:

- notice and transparency – inform data subjects of the items required under the PDPA;
- consent management – obtain and document consent where required;
- purpose limitation – ensure processing aligns with specific, legitimate purposes;
- data accuracy – correct or supplement inaccurate data as needed;
- data security – implement security measures to prevent being stolen, altered, damaged, destroyed or disclosed;
- data subject requests – establish procedures to respond to access, correction, suspension or deletion requests;
- marketing compliance – provide opt-out mechanism for marketing use;
- international transfer – comply with restrictions on cross-border data transfers; and
- (as applicable) – compliance with further sector-specific data protection management and maintenance regulations promulgated by the relevant competent business authority.

1.3 Special Categories of Personal Data

Under the PDPA, medical records, healthcare, genetics, sex life, physical examination and criminal records are considered “sensitive data” and the collection, processing and use of such data must be solely limited to any of the statutory exceptional events – eg, when required by law, when public authorities or private entities are performing statutory duties within a necessary scope, provided appropriate security

measures are taken, or when consent is given by the data subject in writing. Otherwise, the collection, processing and use of such sensitive data shall be prohibited.

1.4 Processing of Personal Data for Research and Development Purposes

In general, companies providing products or services used by healthcare providers shall process and use personal data in compliance with the PDPA.

Regarding processing personal data for research or development purposes, on 2 December 2025, the Legislative Yuan passed the National Health Insurance Data Management Act. Under that act, medical institutions, academic research institutions, universities and legal entities or institutions commissioned by government agencies may apply to use National Health Insurance (NHI) data outside its original statutory purposes (eg, policy analysis or academic research). Such use is limited to public-interest objectives and is subject to strict safeguards, including the requirement that NHI data be de-identified prior to use and that approved use be conducted only within designated secure environments. The use results may not contain any information capable of identifying an individual data subject, and commercial or profit-oriented use is expressly prohibited.

Data subjects have the right to request the cessation of the use for purposes outside the original statutory purposes of all or part of their NHI data. Once recorded, further use for purposes outside the original statutory purposes is prohibited, except for statutory duties by public authorities or urgent threats to life or safety.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

As mentioned in 1.1 Overview of Data and Privacy-Related Laws, the Artificial Intelligence Fundamental Act, which establishes a framework for the development and deployment of AI, was passed by Taiwan’s Legislative Yuan on 23 December 2025.

Under the Artificial Intelligence Fundamental Act, the use of personal data in AI research and applications must comply with privacy-protective principles. Competent authorities are required to consult with the

personal data protection authority to prevent unnecessary collection, processing or use of personal data and to promote the integration of data protection measures by design and by default, thereby safeguarding individual rights throughout the AI lifecycle. This provides specific guidance ensuring that data protection is embedded from the earliest stages of AI system development and deployment.

The regulatory regime is explicitly risk based. A risk classification framework aligned with international standards must be established, and competent authorities are tasked with issuing corresponding risk-based management regulations. High-risk AI applications are subject to enhanced oversight, with certain uses restricted or prohibited under defined conditions. Clear assignment of responsibilities and accountability mechanisms, including remedies, compensation or insurance, are mandated for high-risk AI. Furthermore, government use of AI requires risk assessments and internal control mechanisms proportionate to the nature of the application. Together, these measures ensure that AI deployment and operation uphold data protection obligations, embedding risk mitigation, transparency, human oversight and accountability across the AI lifecycle.

1.6 Data Breach Requirement

In the event that a government or non-government entity becomes aware that personal data it retained has been stolen, altered, damaged, lost or disclosed, the entity is obligated to notify the data subjects concerned.

Where the breach meets specific reporting thresholds, the entity must report the breach to the relevant authorities. The entity must take immediate and effective measures to mitigate the breach, prevent further damage and document the facts, impacts and corrective actions taken. It is also required to retain relevant records for inspection by the supervisory authority.

The specific details regarding the notification process, reporting timelines, scope of reporting, containment measures and record retention shall be subject to rules further established by the supervisory authority. Non-compliance with these obligations may result in the imposition of fines.

In the event of a significant and high-profile data breach, the competent authority is likely to initiate an investigation to determine the cause of the incident and assess whether further action is required, such as holding the responsible parties accountable, imposing fines or requiring the entity to submit corrective action plans.

1.7 Regulators

The PDPC will be the dedicated competent authority of the PDPA. Upon its official launch, the PDPC will integrate those enforcement powers and responsibilities (stated below) spread among the Ministry of Justice (MOJ), the National Development Council, central government authorities that supervise the business operation of non-government agencies, and local government authorities. Further, the PDPC will prioritise the regulation of non-government agencies that do not have a clearly designated competent authority. As for non-government agencies that already have been governed by a competent authority due to the feature of business, transitional provisions will apply. During the transitional period, the supervision by their central or local competent authority will remain in effect temporarily, and the regulatory powers of each respective competent authority will be gradually migrated to the PDPC in phases. This approach aims to achieve the legislative policy goal of centralising and unifying personal data protection oversight.

Before the official launch of the PDPC, the relevant regulators and their authorities are as below.

The MOJ is the main regulator for personal data protection and is in charge of proposing the draft bill of the PDPA, and promulgating the Enforcement Rules of the PDPA (which will be migrated to the PDPC after it is official launched). The MOJ and the National Development Council are in charge of issuing various interpretations to answer questions in respect of compliance with the PDPA.

The enforcement of the PDPA is administered by the central government authorities that supervise the business operation of non-government agencies, and local government authorities. Both central and local government authorities have the power to:

- carry out audits and inspections on non-government agencies;
- request information;
- demand rectification; and
- impose administrative penalties against non-government agencies for non-compliance with the PDPA.

The official establishment of the PDPC is still pending, and it is therefore not yet able to fully exercise the above functions and powers, as the relevant organic law governing its organisation remains under review and discussion. Notwithstanding the foregoing, the PDPC's preparatory office has, in practice, begun to provide certain advisory input on data protection matters to other relevant authorities.

For the typical investigative workflow, please see **1.8 Enforcement Proceedings and Fines**.

1.8 Enforcement Proceedings and Fines **Administrative Investigations and Enforcement**

In the event that a competent authority considers a non-government entity may have violated relevant regulations or deems it necessary to assess the entity's compliance, the authority may initiate an investigation. This investigation typically involves notifying the entity or its personnel to provide necessary explanations, submit required documents, or take other actions for co-operation. The authority may also send personnel to inspect the premises, request explanations from relevant personnel or collect evidence. During such inspections, the competent authority has the right to seize or duplicate any personal data or files that are relevant to the investigation.

Following the investigation, if the competent authority finds no violation, the entity may agree to the publication of such investigation results. If the entity disagrees with the authorities' actions, the entity may file an objection. Where the objection is deemed justified, the authority must modify or suspend the action; otherwise, the authority may proceed with enforcement measures. Should the entity remain dissatisfied with the decision, it may further file an administrative appeal or initiate administrative litigation.

Administrative sanctions for violations of the law include fines, orders to cease the collection, processing or use of personal data, mandatory deletion of personal data files, confiscation or destruction of unlawfully collected data, and public disclosure of the violation and the name of the entity and its responsible persons. Further, administrative fines for violations of the PDPA range from TWD20,000 to TWD15 million.

There are no further explicit unified standards for penalties regarding violation of the PDPA. Nevertheless, as a general rule for administrative control, the fines imposed by administrative authorities shall be in proportion to the degree of violation, and must not involve abuse of discretion or violate the principle of proportionality. The authorities may consider factors such as the circumstances of the violation and frequency of violations when determining the amount of the fine. Based on the limited publicly available information, enforcement of data protection requirements by the Financial Supervisory Commission (FSC), as the competent authority for financial institutions, appears to be relatively more aggressive compared to that of other governmental authorities. With respect to non-financial sector data protection enforcement, where the data breach is serious, involves a substantial volume of personal data, reflects inadequate or sub-standard protective measures, and results in individuals being subject to fraud or scams, the applicable administrative fines are likely to be higher and may exceed TWD1 million.

Criminal Liability

Under the PDPA, a violating person bears criminal liability if they intentionally seek unlawful benefits for themselves or a third party, or intend to harm others, and illegally collect, process, use, alter, delete or otherwise interfere with personal data, including violating statutory obligations or restrictions on international data transfers, thereby causing damage to others. Such conduct may result in imprisonment of up to five years, detention and/or a criminal fine of up to TWD1 million. Where the offender is a public official who commits the offence by abusing their official authority, opportunity or means, the penalty may be increased by up to one-half. The defendant may appeal against the judgment to the High Court, and,

where the statutory requirements are met, may further appeal to the Supreme Court.

In determining the sentence or fine in a criminal case, courts usually consider the nature and seriousness of the offence, the extent of harm or damage caused, the intent and level of fault of the defendant, any illegal benefit obtained, the defendant's personal circumstances, prior criminal record and whether there are mitigating or aggravating factors, so that the punishment is fair and proportionate.

Civil Liability

Under the PDPA, civil liability arises when a government agency or a non-government entity violates the PDPA and causes personal data to be unlawfully collected, processed, used or otherwise infringes upon an individual's rights, resulting in damage. Government agencies are generally liable for damages unless the harm was caused by force majeure, while non-government entities are liable unless they can prove the absence of intent or negligence. Victims may claim compensation not only for property damage, but also for non-property damage, including harm to reputation, and may request appropriate measures to restore reputation. Where actual damages are difficult or impossible to prove, courts may award statutory damages ranging from TWD500 to TWD20,000 per person per incident, subject to an overall cap for mass claims, unless the total harm exceeds that cap. If the party disagrees with the judgment, they may file an appeal.

When determining the amount of compensation in a civil case, courts generally consider the nature of the wrongful conduct, the extent of actual damage suffered by the victim, the degree of intent or negligence of the wrongdoer, and the economic circumstances of the parties.

1.9 Enforcement Trends

Severe Administrative Fines Against Financial Institutions for Data Protection Violation Remains Unchanged

On 9 December 2025, an employee of the CTBC Bank, acting without any business-related necessity, privately accessed and queried customers' personal data through the bank's internal systems. The Finan-

cial Supervisory Commission (FSC) determined that the CTBC Bank had deficiencies in its protection of customers' personal data and had failed to properly implement its internal control system. On this basis, the FSC imposed an administrative fine of TWD2 million on the CTBC Bank.

Severe Administrative Fines Against Non-Financial Institutions for Data Protection Violation

On 19 June 2024, a chain fitness company, WorldGym, and its legal representative – ie, the Chairman of the company, were each fined TWD1.4 million by the authority for:

- failing to implement appropriate security measures, which led to a personal data breach (TWD1.2 million); and
- failing to notify the affected data subjects after the data breach (TWD0.2 million).

The reasons that the fitness company and its legal representative were subject to the severe fines include that the company has been classified by the National Police Agency as a “high-risk business”, indicating a heightened vulnerability to personal data breaches that could be exploited by scam groups to carry out scams against the public, and, in this case, individuals were also reportedly defrauded by scam groups using the leaked personal data, resulting in actual financial damages/losses.

Proactive Administrative Investigation Against High-Profile Data Incidents

Since late 2024, the competent authorities have adopted a practice of proactively initiating investigations into high-profile personal data incidents, regardless of whether such incidents occur domestically or overseas. Where a reportedly serious data incident occurs outside Taiwan but involves, or may involve, personal data of individuals in Taiwan, the relevant Taiwan authority will proactively commence an investigation against the related Taiwan entity.

By way of example, a widely used social media platform across Taiwan, Japan, Korea and other Asian jurisdictions was reported to have suffered a serious data incident involving approximately 440,000 personal data records, more than 100 of which were

related to Taiwan individuals. In response, the competent authority, the Ministry of Digital Affairs, proactively initiated an intensive investigation into the group's Taiwan presence. Similarly, in 2025, certain systems of well-known luxury brands were reportedly hacked overseas, potentially affecting a substantial volume of Taiwan personal data, and the Ministry of Economic Affairs likewise launched investigations into such incidents to clarify the impact on Taiwan personal data as well as the data protection compliance of its relevant Taiwan presences.

These developments demonstrate a shift in the authorities' enforcement approach toward a more proactive and assertive stance in the enforcement of data protection laws.

Practical Takeaways for Organisations

In line with global data protection trends and efforts to prevent the unlawful use of leaked data, Taiwan authorities have adopted a more proactive and assertive approach to the enforcement of data protection laws. In addition, they have begun to conduct more intensive investigations and to impose more stringent sanctions where violations are identified in the end. In light of these developments, enterprises, regardless of acting as data collectors, processors and/or controllers, are advised to strengthen their data protection governance, internal controls and overall compliance frameworks.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Trends in Data Breach Litigation Related to Fraudsters Exploiting Leaked Personal Data

In Taiwan, cases of fraudsters exploiting leaked personal data to scam data subjects have become increasingly prevalent. There is a growing trend of data subjects, who suffer both material and non-material damage, seeking compensation from the businesses responsible for the data breaches. The majority of courts held that the material damage suffered by the data subjects is a result of the fraudsters' actions, not those of the business, and therefore, no causation exists between the data breach and the material damage. However, some of them further held that the

emotional distress suffered by the data subjects in the fraud event is linked to the business's data breach, allowing data subjects to seek compensation for non-material damage. When claiming non-material damages, the claimant must substantiate the nature of the harm suffered. For example, in cases where the victim's personal data is leaked, resulting in fraud by fraudsters, the courts have recognised that the data breach and subsequent fraud caused the claimant emotional distress, thus justifying compensation for non-material damages. Where such non-material damages are difficult or impossible to prove, the court may award statutory damages of up to TWD20,000 per data subject per incident. While this amount may appear modest on an individual basis, the aggregate exposure could be substantial in the context of mass claims or class actions.

2.2 Recent Case Law

Case Regarding Right to be Forgotten

A well-known case is one in which a former professional baseball CEO claimed the right to be forgotten and requested Google Inc. to remove search results related to his match-fixing scandal. This case began in 2017, and has been heard by the district court, the High Court and the Supreme Court. The Supreme Court has twice remanded the case for re-examination by the High Court. In these judgments, the courts generally recognise that the right to be forgotten falls within the scope of privacy rights and is protected under the Constitution. However, search engine operators' provision of search results, although commercially driven or for profit, should still be protected under the freedom of speech protected by the Constitution. Such search results should not be arbitrarily restricted or deleted, as doing so would undermine the performance freedom and neutrality of search engine operators which could, in turn, affect the public's perception and judgement, and even threaten the foundation of democratic constitutionalism. Therefore, when determining whether certain search results should be deleted, courts seek to strike a balance between public interest and privacy rights. The Supreme Court restated the foregoing view and opined that the data subject may also request the deletion of the collected or processed data if there is a more significant interest that needs to be protected. This includes many factors such as whether the data subject is a public figure,

and whether the data has been outdated or causes disproportionate negative privacy impacts on the data subject. The Supreme Court also considers whether the deletion would affect or hinder the public's right to know.

From the above, it is clear that the courts attempt to balance public interest with privacy rights. In deciding whether specific search results should be deleted, the High Court and the Supreme Court have reached different conclusions based on the consideration of those factors. The match-fixing scandal was 14 years ago. At the second review of the Supreme Court in 2024, it dismissed the judgment of the High Court again and requested the High Court to reconsider and seek a balance between the right to be forgotten and the public's right to know based on all the relevant factors.

Taken together, these judgments have significantly shaped the framework for privacy-related litigation in Taiwan, particularly with respect to the right to be forgotten. The courts apply a contextual balancing test between privacy rights and competing constitutional interests, notably freedom of speech and the public's right to know. Rejecting any automatic right to deletion, the courts assess factors such as the data subject's public status, the passage of time, ongoing relevance, proportionality of the privacy impact and the effect of deletion on public discourse. Accordingly, the right to be forgotten is subject to judicial scrutiny rather than automatic enforcement.

2.3 Collective Redress Mechanisms

Collective Redress Mechanisms – Class Action

The PDPA provides a collective redress mechanism through class actions for data protection violations. For cases caused by the same cause and fact, and where multiple data subjects are infringed, the organisations regulated by the PDPA may – after obtaining a written authorisation of litigation rights of 20 or more data subjects – represent such data subjects in bringing a lawsuit to the competent court in its own name. Regarding class action, the legislation does not provide a specific timeline for the completion of judicial proceedings. However, in the first data breach class action case (please see below for details), the court took approximately eight months to render a

first-instance judgment, after which the parties settled during the appellate proceedings.

The First Data Breach Class Action

The first personal data infringement class action was brought by the Consumers' Foundation against a travel agency in March 2018, with the court rendering its decision in October 2019.

In this case, the Consumers' Foundation claimed TWD4,509,575 compensation on behalf of 25 consumers, on the grounds that a travel agency leaked the personal data collected and thus caused damages to the consumers. The travel agency countered that the data breach was caused by a malicious hacking attack, and that it had notified the data subjects of the data breach after the occurrence of such attack; therefore, it should not be held liable for the data breach.

The court rendered a judgment in favour of the defendant, opining that the travel agency had established a security and maintenance plan for the protection of personal data files, and that it had conducted internal audits, education and training for cybersecurity personnel, and changed the passwords for the computer system periodically.

Therefore, although there was a data breach caused by a hacking attack, the court held that the travel agency was not in violation of the PDPA and thus should not be held liable for the data breach. The Consumer Foundation has filed an appeal against this judgment. During the procedure in the court of second instance, the Consumers' Foundation and the travel agency reached a settlement.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

In Taiwan, there is currently no unified law specifically governing cross-sector data access and data-sharing frameworks in the context of emerging technologies such as the Internet of Things and cloud computing. Nevertheless, in response to the rapid development of AI and the indispensable role of data in AI training and applications, a draft Data Innovation and Utiliza-

tion Promotion Act has been proposed and is presently under deliberation by the Legislative Yuan. The draft bill aims to facilitate the circulation and utilisation of data, enhance national competitiveness in the digital domain and promote data-driven innovation by encouraging the opening and sharing of data. Under the draft, data may be classified and made available as “open data” or “shared data” in accordance with applicable licensing and usage conditions for the purpose of promoting data innovation and utilisation. Nevertheless, where such data involves personal data, it still must be governed by and processed in compliance with the PDPA. Government agencies, with respect to the government data under their control, are required to promote data innovation and utilisation within the scope of their respective statutory functions pursuant to the draft legislation, and to periodically review their implementation to ensure compliance with the PDPA, the Cyber Security Management Act, the Trade Secrets Act, the Copyright Act and other relevant laws. In addition, the draft empowers government agencies to encourage inter-industry co-operation to establish secure, accessible and interoperable data-sharing mechanisms, and to promote the voluntary sharing of industry-held data under fair, reasonable and non-discriminatory data-sharing terms.

The draft Data Innovation and Utilization Promotion Act is currently under legislative review, and its final provisions and regulatory framework have not yet been determined. Upon enactment, the Act is expected to establish a legal foundation for data sharing and utilisation while ensuring compliance with personal data protection, cybersecurity and other applicable legal requirements.

3.2 Interaction of Data Regulation and Data Protection

Pursuant to the draft Data Innovation and Utilization Promotion Act, the promotion of data sharing and utilisation is intended to facilitate innovation and support applications such as AI; however, such activities remain subject to the continued applicability of existing legal regimes. The processing of personal data must adhere to the requirements of the PDPA, including the establishment of a lawful basis, observance of purpose limitation and the implementation

of appropriate security measures. Similarly, non-personal data, including information potentially protected under intellectual property or trade secret laws, must be managed in accordance with all relevant legal obligations, so as to prevent infringement of proprietary rights. In this manner, the draft legislation seeks to enable the circulation and innovative use of data while ensuring ongoing compliance with established statutory protections governing privacy, cybersecurity and intellectual property.

3.3 Rights and Obligations Under Applicable Data Regulation

Under the draft Data Innovation and Utilization Promotion Act, government agencies may provide open data (ie, data that is licensed for use without limitation as to purpose, geographic region or duration, and is provided in a machine-readable, widely accepted format) in accordance with principles of searchability, accessibility, interoperability and reusability, and must provide metadata or explanatory information to facilitate interpretation. They are also required to maintain the integrity, accuracy, usability and timeliness of open data, and may encourage inter-industry co-operation to establish secure, accessible and interoperable data-sharing mechanisms. Shared government data (ie, government data that is shared and licensed for use under specific conditions, including the right of the licensor to withdraw the authorisation) must be provided on a non-exclusive basis under fair, reasonable and non-discriminatory conditions, unless justified by public interest.

Personal data may only be shared or utilised in compliance with the PDPA, with appropriate safeguards to ensure security and lawful processing. In the context of the data altruistic mechanism, only government agencies or non-profit entities are permitted to act as operators, and such operators must possess adequate technical and organisational capacity in information security and personal data protection to safeguard individuals' personal data and maintain cybersecurity. Any sharing or use of personal data must be accompanied by appropriate protection mechanisms, in accordance with guidelines to be issued by the competent personal data protection authority. The competent authority shall also prescribe the operational procedures of the mechanism, includ-

ing registration and termination of operators and other relevant matters.

Accordingly, organisations acting as data altruistic operators should therefore assess their eligibility, establish the necessary technical and organisational capabilities, register with the competent authority, implement internal processes to manage authorisations, and adopt measures to protect personal data in accordance with regulatory guidelines. As the detailed operational rules and protective measures have not yet been fully clarified, the precise obligations of organisations will become clearer once these provisions are established.

3.4 Regulators and Enforcement

In general, the competent authority of the draft Data Innovation and Utilization Promotion Act is the Ministry of Digital Affairs, which is responsible for overseeing the operation of the data altruistic mechanism, including registration, termination and related procedures of operators. For matters relating to the protection of personal data, the competent authorities (eg, the PDPC) will be responsible for issuing guidelines to ensure that personal data involved is properly safeguarded. The Ministry of Digital Affairs co-ordinates with the personal data protection authority to ensure compliance with the PDPA, and the draft law's requirements for non-exclusive and non-discriminatory data sharing reflect the need to avoid unfair practices and restrictions on competition.

As this draft Act remains a draft and the related subordinate regulations have not yet been established, the operational framework will be more clearly defined once these provisions are formally issued.

4. Sectoral Topics

4.1 Use of Cookies

The PDPA does not have specific provisions directly addressing cookies, SDKs and other device identifiers. Nevertheless, their use, which typically involves collecting personal data from users' devices, must comply with the general principles of the PDPA. This includes:

- providing certain information required by the PDPA, such as the name of the business, the types of personal data being collected, the rights of the data subjects, and the duration, location, recipients and methods of data use, and this information is usually provided in the form of a cookie policy or privacy notice;
- obtaining informed consent from data subjects;
- ensuring that data is used only for specified purposes within the scope of data subjects' consent;
- implementing appropriate security measures to protect personal data; and
- respecting data subjects' rights, such as to access, rectify, delete, or request a copy of their personal data, or demand the cessation of the collection, processing or use of their personal data.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised or Targeted Advertising

Personalised or targeted advertising is not specifically regulated under a separate legal framework in Taiwan, but it is governed by the general provisions of the PDPA. Since personalised or targeted advertising often involves the collection and analysis of personal data to target individuals with tailored ads by way of collecting and analysing the browser records and footprint and at least partial IP information, it must comply with the requirements set out in the PDPA (please refer to 4.1 Use of Cookies). Therefore, businesses engaging in personalised or targeted advertising must adhere to the PDPA's general data protection principles to ensure legal compliance. This includes adhering to the requirements when performing profiling and ensuring that, if sensitive data is involved, the collection, processing and use of such data fully comply with the legal requirements for handling sensitive data (please refer to 1.3 Special Categories of Personal Data).

Other Online Marketing Practices

The PDPA regulates the collection and use of personal data for marketing purposes. When a non-governmental agency uses personal information for the purpose of marketing but the data subject refused the marketing, such marketing must stop immediately. Also, the non-governmental agency should offer ways for the data subject to express their refusal at

the time such marketing first appears in public, and should compensate any necessary cost and expense for expressing such refusal.

Moreover, the Financial Holding Company Act provides that financial holding companies' subsidiaries engaging in co-selling activities among themselves should apply to the FSC for prior approval and ensure that such activities will not harm the interests of customers. The subsidiaries of the financial holding company should comply with the provisions of the PDPA with regard to the joint collection, processing and use of the basic personal data and dealing or transaction records of customers.

In Taiwan, there are no general and primary rules regulating all types of online marketing. Nevertheless, for electronic marketing, the Consumer Protection Committee has promulgated guidance advising that enterprises collect and use consumers' personal information in accordance with the law, and provide reasonable protective measures.

4.3 Employment Privacy Law

In addition to the PDPA, which plays a primary role in data privacy, in employment relationships, the relevant labour laws provide further rules. According to the Employment Service Act and its enforcement rules, when recruiting or hiring employees, an employer may only request "privacy data" that is necessary and related to the employment relationship, while respecting the employee's rights. The information requested must be legitimate, necessary and reasonably related to specific economic needs or public interests. "Privacy data" includes physiological data (such as genetic testing, drug testing, HIV testing, etc), psychological data (such as psychological tests, lie detector tests, etc), and personal life information (such as credit records, criminal records, background checks, etc). However, the employer is prohibited from requesting personal information that is not relevant to employment, as well as from retaining the employee's ID, work certificates or other documents not required for employment purposes. In other words, all requests must be strictly limited to information necessary for the employment process and aligned with legitimate economic purposes.

In practice, for the employment privacy issues (such as email monitoring, installing surveillance cameras in the workplace, recording employees' activities within the office, or capturing their computer screen activities), Taiwan courts use the following standards to determine whether the measure is in violation of employees' privacy rights:

- necessity of the purpose – whether the measure is implemented for a legitimate business purpose;
- proportionality of the method – whether the method used is appropriate and does not exceed what is necessary to achieve the legitimate business goal; and
- balancing of interests – using the least intrusive means to achieve the business objective.

By way of example, in cases involving email monitoring, certain court rulings have indicated that where a company has implemented an email policy clearly stating that employees' emails may be monitored, or where employees have provided written consent to such monitoring, it is difficult to conclude that employees retain a reasonable expectation of privacy in those emails.

4.4 Data Protection in M&A

In M&A and asset transactions, privacy and data protection are critical considerations throughout the entire transaction lifecycle, from due diligence to post-closing integration. During the due diligence phase, existing privacy and data protection compliance should be reviewed regardless of whether the target operates in a data-rich industry, although data-intensive businesses are typically subject to heightened scrutiny due to more stringent and complex regulatory requirements. In certain industries, such as big data, data analytics or other emerging data-driven businesses, it is often fundamental to assess whether the relevant datasets constitute personal data and to evaluate how such data is collected, processed and utilised. In this context, it is also necessary to precisely identify the role played by the target, including whether it acts as a data collector, processor and/or controller, so as to precisely clarify the compliance status in all material aspects. Such assessments typically require close and co-ordinated collaboration between technical and legal teams.

In addition, the PDPA and related regulations govern change-of-control arrangements, data transfers and post-closing integration activities involving personal data. By way of example, where a proposed transaction involves the transfer of personal data, key matters to be considered and addressed include the categories of data involved, the destination of the transfer and the applicability of any required notices, consents and/or regulatory approvals etc.

5. International Considerations

5.1 Restrictions on International Data Transfers

For personal data, under the PDPA, “cross-border transfer” refers to the cross-border processing or use of it. In general, cross-border transfer of personal data is permitted, while the government authority in charge of the pertinent industry may, at its reasonable discretion, impose limitations on international data transfers if:

- they involve important national interests;
- a national treaty or agreement specifies otherwise;
- the country receiving the personal information lacks proper regulations towards the protection of personal information and it might harm the rights and interests of the data subject; or
- international transfers of personal information are made through an indirect method in which the provisions of the PDPA may not be applicable.

Pursuant to the above provision and relevant laws governing particular industries, certain authorities further promulgate and require certain data residency/data localisation requirements whose nature will impose certain restrictions on international data transfer. For example, the FSC promulgates certain data residency requirements for financial institutions.

In addition, certain authorities promulgate and impose restrictions in terms of which certain specific industries are prohibited from transferring data to a specific territory. For example, communications enterprises, social worker offices or human resource agencies are prohibited by respective governmental authorities in

charge of the pertinent industry from transferring their subscribers’ or their clients’ personal data to China.

With respect to non-personal data, there is currently no unified or dedicated legislation in Taiwan that specifically governs the details of cross-border data transfers. However, consistent with the global trend toward strengthening the protection of national security and critical technologies, Taiwanese laws – including the National Security Act, the Trade Secrets Act and other relevant legislation – may apply to prevent the unlawful disclosure or leakage of such data to restricted territories, foreign hostile forces or any persons or entities controlled by them. Violations of these laws may give rise to severe criminal liability.

5.2 Government Notifications and Approvals

The relevant competent authority may promulgate sector-specific rules governing international data transfers for a specific industry. For example, as described in **5.1 Restrictions on International Data Transfers**, the laws and regulations impose a localisation principle for customers’ finance records. If a financial institution wishes to outsource its data entry, processing and the output operations of an information system related to consumer finance business to an offshore service provider, it must submit the application with required materials, including the internal outsourcing guidance and board resolution which allows and approves such international transfer, and necessity analysis and corresponding rules and plan for subsequent management and emergency handling, etc, to the FSC for approval.

With respect to non-personal data, Taiwanese laws and regulations also impose certain management and control measures. In particular, prior approval from the Department of Investment Review of the Ministry of Economic Affairs is required where a Taiwanese individual or legal entity intends to transfer or license its technology, patents, know-how or other intellectual property, whether or not registered with the relevant authority, to a China individual or entity. Further, the amendments to the Industrial Innovation Statute, which came into effect on 7 May 2025, reflect the global trend toward enhanced protection of critical technologies and significantly strengthen the regulatory framework governing outbound investments by

domestic companies. Under the amended regime, not only outbound investments meeting prescribed transaction value thresholds, but also investments involving designated countries or territories, or specified industries or technologies, are subject to prior approval by the competent authority. In conducting its review, the authority will assess, among other factors, the potential impact of the proposed investment on national security and economic development. Taken together, these regulations indicate that Taiwanese laws and regulations are evolving toward a more comprehensive and substantive framework for the protection of non-personal data, particularly from the perspective of technology and national security protection.

5.3 Data Localisation Requirements

As stated in **5.1 Restrictions on International Data Transfers**, international data transfers are in general permitted by the PDPA, while it leaves the room and flexibility to the relevant competent authority to impose restrictions at its discretion based on the regulation and management needs of the specific industry. Therefore, the relevant competent authority may still promulgate sector-specific rules governing data localisation for a specific industry. Please see **5.1 Restrictions on International Data Transfers** and **5.2 Government Notifications and Approvals** for details.

The current regulatory regime is silent as to whether remote access constitutes a “transfer” and the relevant authorities have not provided written interpretation for this matter, although it seems that this may be the case. This view relies on a boarder interpretation of the PDPA, under which an “international transfer” is defined to include cross-border “processing” or “use” of personal data. If so characterised, the regulatory requirements applicable to cross-border transfers under the PDPA would correspondingly apply to scenarios involving remote access. In light of this evolving regulatory stance, cross-border enterprises are advised to closely monitor further developments on this issue and evaluate any potential impacts which might impact their global and cross-border data protection structure, designs and measures.

5.4 Blocking Statutes

In Taiwan, cross-border disclosures or foreign discovery requests are subject to restrictions under the PDPA, when personal data is involved. Execution of foreign-court judgments in Taiwan typically requires going through procedures under Taiwan laws. Recognition of foreign judgments is governed under the Code of Civil Procedure, which requires proper jurisdiction, due process, public policy compliance and reciprocity.

Additionally, national security laws (eg, the National Security Act) may restrict cross-border disclosures or co-operation if the information relates to national security matters.

5.5 Recent Developments

In addition to those described in **5.1 Restrictions on International Data Transfers** to **5.3 Data Localisation Requirements**, on 30 September 2025, the Ministry of Health and Welfare announced “the restriction on the international transfer of personal data by the wholesale and retail pharmaceutical industry to China, Hong Kong, and Macau”. It is stipulated that the wholesale and retail pharmaceutical industry shall not transfer the personal data it collects, processes and uses to China, Hong Kong and Macau unless an exception applies. This regulation will take effect on 1 October 2026 to govern specific pharmaceutical wholesale and retail operators and will extend to all pharmaceutical wholesale and retail operators from 1 October 2027.

THAILAND



Law and Practice

Contributed by:

Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn
Chandler Mori Hamada Limited

Contents

1. Legal and Regulatory Framework p.493

- 1.1 Overview of Data and Privacy-Related Laws p.493
- 1.2 Rights and Obligations p.494
- 1.3 Special Categories of Personal Data p.495
- 1.4 Processing of Personal Data for Research and Development Purposes p.495
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.496
- 1.6 Data Breach Requirement p.496
- 1.7 Regulators p.496
- 1.8 Enforcement Proceedings and Fines p.497
- 1.9 Enforcement Trends p.497

2. Privacy Litigation p.498

- 2.1 Privacy Litigation Overview p.498
- 2.2 Recent Case Law p.499
- 2.3 Collective Redress Mechanisms p.499

3. Requirements for the Protection and Processing of Non-Personal Data p.499

- 3.1 Objectives and Scope of Data Regulation p.499
- 3.2 Interaction of Data Regulation and Data Protection p.499
- 3.3 Rights and Obligations Under Applicable Data Regulation p.499
- 3.4 Regulators and Enforcement p.499

4. Sectoral Topics p.499

- 4.1 Use of Cookies p.499
- 4.2 Personalised Advertising and Other Online Marketing Practices p.500
- 4.3 Employment Privacy Law p.500
- 4.4 Data Protection in M&A p.500

5. International Considerations p.501

- 5.1 Restrictions on International Data Transfers p.501
- 5.2 Government Notifications and Approvals p.501
- 5.3 Data Localisation Requirements p.501
- 5.4 Blocking Statutes p.501
- 5.5 Recent Developments p.501

Contributed by: Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn,
Chandler Mori Hamada Limited

Chandler Mori Hamada Limited combines an international standard of practising law with decades of local experience in the Thai legal environment. The team of more than 100 lawyers in Thailand is internationally recognised for its legal expertise in anti-trust and competition, aviation, banking and project financing, capital markets, corporate and M&A, data

privacy and data protection, dispute resolution, energy, natural resources and infrastructure, insurance, labour and employment, real estate, REITs, regulatory and public policy employment and tax, restructuring and insolvency and technology, and media and telecommunications.

Authors



Jutharat Anuktanakul is a partner at Chandler Mori Hamada. She has represented Thai and international clients in preparing applications for investment promotion to the Board of Investment and the Industrial Estate

Authority of Thailand in a wide variety of sectors, including energy, telecommunications, electronics and software. As a specialist in corporate law, she has represented numerous clients in share or asset acquisitions, partial and complete business transfer transactions, and registration of regional, branch and representative offices of foreign corporations. Jutharat also advises on other regulatory and data protection compliance strategies.



Suphakorn Chueabunchai is a senior associate at Chandler Mori Hamada. He specialises in corporate and regulatory matters, with experience in advising on mergers and acquisitions and due diligence of Thai target

companies. He also has significant experience in privacy and data protection law, advising leading clients on PDPA compliance and conducting gap analyses across the financial services, modern trade, automotive and pharmaceutical sectors. In addition, Suphakorn advises digital platforms and e-commerce businesses on regulatory compliance, including licensing requirements and applicable laws.



Pitchaya Roongroajsataporn is an associate at Chandler Mori Hamada and a member of the corporate and mergers & acquisitions practice group. She has a particular focus on the technology, media and

telecommunications (TMT) sector, including data protection. Her experience includes advising on a broad range of data protection issues, including the PDPA in Thailand, applying for digital asset business licences and providing regulatory advice related to the technology sector.

Chandler Mori Hamada Limited

31st and 36th Floors
Sathorn Square Office Tower
98 North Sathorn Road
Silom
Bangrak
Bangkok 10500
Thailand

Tel: +662 009 5000
Fax: +662 009 5080
Email: business-development@morihamada.com
Web: chandler.morihamada.com

CHANDLER
MORI HAMADA

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Personal Data Protection Act B.E. 2562 (2019) (PDPA) is the primary law regulating the processing of personal data in Thailand. As in other jurisdictions, “personal data” is defined as any data which, by itself or in combination with other data, can be used to identify an individual, excluding data relating to deceased persons in particular.

The PDPA focuses on the protection of data subjects whose personal data is processed, including through collection, storage, use, disclosure and other forms of processing, regardless of the original source of such personal data. Entities that determine the purposes and means of processing personal data (known as “Personal Data Controllers” or “controllers” under the PDPA) are required to have a lawful basis for processing any personal data and to maintain proper security measures to prevent any loss, unauthorised access, use or disclosure of personal data. These requirements also apply to service providers that process personal data as instructed by or on behalf of a controller (known as “Personal Data Processors” or “processors” under the PDPA).

The PDPA is based mainly on the EU General Data Protection Regulation (GDPR), and imposes obligations on the private sector and government bodies (ie, both Personal Data Controllers and Personal Data

Processors) regardless of the mode of processing (ie, both automated and non-automated processing), especially regarding burden of proof.

The PDPA itself applies to most activities, subject to certain exemptions, such as:

- household activities;
- the operation of public authorities for public safety purposes; and
- media and fine arts activities carried out in accordance with professional ethics.

For businesses regulated by specific supervisory authorities (such as banks and insurance businesses), the PDPA allows those supervisory authorities to issue the standard forms or guidelines for their operators to follow.

The PDPA has explicit extraterritorial reach. If a controller/processor is outside Thailand, the PDPA can still apply if the relevant personal data relates to data subjects in Thailand, and the activities involve either:

- the offering of goods or services to individuals in Thailand (irrespective of whether payment is required); or
- the monitoring of behaviour that takes place in Thailand.

In this regard, the PDPA operates alongside other laws governing non-personal data and cybersecurity, and

generally applies as a supplementary framework to such laws. Certain sector-specific or special laws may impose stricter requirements relating to security, governance or compliance than those prescribed under the PDPA. Accordingly, organisations must assess on a case-by-case basis whether any specific or industry-related laws apply to their operations, and ensure compliance with the higher or more stringent standards where applicable.

1.2 Rights and Obligations

The general principles for the processing of personal data under the PDPA are broadly aligned with the seven principles of the GDPR, and can be summarised as follows.

- Lawfulness, fairness and transparency – personal data must be processed lawfully, fairly and transparently, with clear information provided to data subjects.
- Purpose limitation – personal data must be collected for specific and legitimate purposes and not used beyond those purposes, unless permitted by law.
- Data minimisation – only personal data that is necessary for the stated purpose may be collected and processed.
- Accuracy – personal data must be accurate, up to date, and corrected where necessary.
- Storage limitation – personal data must not be retained longer than necessary, unless retention is required by law.
- Integrity and confidentiality (security) – appropriate technical and organisational measures must be in place to protect personal data.
- Accountability – data controllers are responsible for PDPA compliance and must be able to demonstrate such compliance.

Lawful Bases for Processing Personal Data Under the PDPA

Under the PDPA, personal data may be processed only where a lawful basis applies. If no lawful basis is available, consent must be obtained.

Key lawful bases include the following.

- Consent – freely given, informed and explicit (especially for sensitive personal data).
- Research and statistics – necessary for research or statistical purposes, subject to appropriate safeguards for data subjects' rights and freedoms.
- Contractual necessity – necessary for entering into or performing a contract with the data subject.
- Legal obligation – necessary to comply with applicable laws.
- Vital interests – necessary to prevent danger to life, body or health.
- Public task/public interest – necessary for tasks carried out in the public interest or under official authority.
- Legitimate interests – necessary for legitimate interests of the controller or a third party, provided such interests do not override the data subject's fundamental rights and freedoms.

Data Subject Rights Under the PDPA

Under the PDPA, data subjects are entitled to the following rights.

- Right of access – to request access to and obtain a copy of their personal data.
- Right to rectification – to request correction of inaccurate or incomplete personal data.
- Right to erasure (right to be forgotten) – to request deletion or anonymisation of personal data when it is no longer necessary or unlawfully processed.
- Right to restriction of processing – to request temporary suspension of processing in specific circumstances.
- Right to data portability – to request personal data in a structured, commonly used and machine-readable format, where applicable.
- Right to object – to object to processing based on legitimate interests, direct marketing or other grounds prescribed by law.
- Right to withdraw consent – to withdraw consent at any time, without affecting prior lawful processing.
- Right to lodge a complaint – to lodge a complaint with the Personal Data Protection Committee (PDPC).

Main PDPA Compliance “To-Dos” for Organisations (as Data Controllers)

The primary compliance requirements are as follows:

- identifying and documenting all personal data processing activities;
- determining and recording the lawful basis for each processing activity;
- preparing and maintaining PDPA-compliant privacy notices;
- establishing procedures for handling data subject rights requests;
- implementing appropriate technical and organisational security measures;
- managing third parties through data processing agreements; and
- training employees on PDPA compliance and data protection awareness.

1.3 Special Categories of Personal Data

Under the PDPA, “sensitive personal data” includes personal data relating to the following matters, among others:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- sexual behaviour;
- criminal convictions;
- health data, disability and genetic data;
- biometric data; and
- trade union membership.

The processing of sensitive personal data is prohibited by default, unless a specific legal basis applies.

Permitted Grounds for Processing

Sensitive personal data may be processed only where one of the following applies.

- Explicit consent – consent must be explicit, informed and specific, and must be clearly distinguishable from other matters.
- Vital interests – necessary to prevent or suppress danger to the life, body or health of a person, where the data subject is incapable of giving consent.

- Legal obligations – required for compliance with laws relating to labour protection, social security or other statutory duties.
- Public interest/official authority – necessary for the performance of duties carried out in the public interest or for the exercise of official authority.
- Medical and public health purposes – necessary for preventative medicine, medical diagnosis, healthcare services or public health, subject to appropriate safeguards.
- Research or statistical purposes – necessary for research or statistics, provided suitable measures are in place to protect data subjects’ rights and freedoms.

Additional strict security measures must be implemented when processing sensitive personal data. In particular, personal data relating to criminal convictions or criminal offences is subject to specific sub-regulations under the PDPA. Such data may be collected and retained only to the extent necessary or as required by law, and must not be retained for more than six months from the date of collection, unless otherwise permitted or required by applicable law.

Personal Data Relating to Minors

Under the PDPA, a minor is a person under 20 years of age, unless legally married.

Consent requirements

- Where consent is relied upon as the lawful basis for processing, consent must be obtained from the parent or legal guardian.
- If the minor is under ten years of age, parental or legal guardian consent is required in all cases.
- If the minor has legal capacity under applicable law, consent may be obtained directly from the minor.

Controllers must exercise heightened care when processing minors’ data, ensuring transparency, fairness and security, and avoiding unnecessary or excessive data collection.

1.4 Processing of Personal Data for Research and Development Purposes

Under the PDPA, truly anonymised data (ie, data that can no longer identify a natural person, whether direct-

ly or indirectly) falls outside the scope of the PDPA. Once data is irreversibly anonymised, it is no longer considered personal data and may be used without relying on a lawful basis under the PDPA. However, the process of anonymisation itself involves the processing of personal data (and often sensitive health data) and must therefore comply with the PDPA until anonymisation is completed.

Note that health data may be processed without consent where the processing is:

- necessary for medical purposes, public health, scientific research or statistics, as authorised by applicable laws; and
- subject to appropriate safeguards to protect data subjects' rights and freedoms, such as data minimisation, access controls and security measures.

This exemption may apply where companies act on behalf of healthcare providers (eg, as data processors) in connection with healthcare systems or medical technologies.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

At present, Thailand does not have a specific or binding AI law governing the use of personal data in AI systems or automated decision-making. As a result, the processing of personal data in AI models is regulated primarily under the PDPA, and organisations must comply with general data protection principles such as lawfulness, purpose limitation, data minimisation, transparency, security and accountability.

The PDPA does not establish a dedicated risk-based classification for AI systems, nor does it prohibit specific AI use cases. In practice, organisations are expected to adopt a risk-based approach, especially where AI involves large-scale processing, sensitive personal data, or automated decision-making with significant effects. Regulators have recommended conducting Data Protection Impact Assessments (DPIAs) as a key tool to identify and mitigate privacy risks. Transparency regarding AI use, sound data governance and appropriate human oversight are therefore treated as regulatory expectations rather than strict statutory requirements.

1.6 Data Breach Requirement

Under the PDPA, where a personal data breach occurs, the data controller must act without delay and, in any event, notify the PDPC within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to data subjects' rights and freedoms. The controller must first identify the nature and cause of the breach and assess the associated risks, taking into account factors such as the type and sensitivity of the data involved, the number of affected data subjects, the likelihood of misuse, and the potential impact on individuals. Where the breach is likely to result in a high risk, affected data subjects must also be notified without undue delay. The controller must then implement remedial and mitigation measures, including containment and recovery actions, and establish preventative measures to avoid recurrence. The PDPC has the authority to investigate data breaches, request information and impose administrative sanctions. In addition, affected data subjects may bring civil claims, including collective or mass actions, for damages arising from PDPA violations.

In this regard, over the past year the PDPC has adopted a more proactive and assertive enforcement approach. Where a data breach is reported or detected through dark web disclosures or public discussions on social media, the PDPC may initiate inquiries and summon the organisation to provide explanations and information, even before a formal notification is submitted. In some cases, such summonses have been publicly announced through the PDPC's official social media platforms, increasing reputational and regulatory exposure. As a result, organisations are expected to exercise heightened caution and preparedness in managing data breach risks, including timely internal assessments, clear communication strategies and well-documented response measures.

1.7 Regulators

The PDPC is the supervising authority under the PDPA. The PDPA also established the Office of the PDPC to support the PDPC in developing and facilitating enforcement. Under the PDPA, the PDPC has several duties, such as:

- ensuring the preparation and implementation of the master plan for the promotion and protection of personal data;
- promoting and supporting government agencies and the private sectors in evaluating the operational results of such master plan;
- determining measures or guidelines relating to data protection operations in order to comply with the PDPA;
- issuing notifications or rules for the implementation of the PDPA; and
- providing advice or consultancy to any persons.

In addition, the PDPC shall appoint expert committees to consider any complaints under the PDPA, including investigating any acts in connection with personal data, settling disputes and carrying out other tasks assigned by the PDPC.

1.8 Enforcement Proceedings and Fines

As mentioned in 1.7 **Regulators**, an expert committee is responsible for considering and investigating any complaints on behalf of the PDPC in accordance with the PDPC's rules. If any complaint does not comply with such rules, the expert committee will not accept such complaint for consideration.

If, following consideration or investigation, the expert committee finds that such complaint is capable of settlement and the relevant parties are willing to settle, the expert committee must proceed with dispute settlement before issuing any order mandating the operator (whether the controller or processor) to perform or rectify their act, or prohibiting the operator from carrying out an act that would cause damage to a data subject.

If the operator fails to comply with the expert committee's order, administrative procedures will be applied (including powers to order seizure, attachment and sale by auction, as allowed by law). The expert committee's order is final, although any party may appeal such order in accordance with administrative procedure within 15 days of receiving such order.

In this regard, a PDPC Notification on Administrative Penalties governs the enforcement of administrative penalties and sets out the criteria for how administra-

tive penalties (as determined by the expert committee) are used. The expert committee will determine and apply administrative penalties based on the seriousness of such offence. Offences are categorised into two groups: serious and non-serious offences. Under the Notification on Administrative Penalties, the expert committee is empowered to impose administrative penalties accordingly.

Serious Offences

The expert committee can impose administrative fines on a controller and/or processor. In addition, administrative fines can be imposed on offenders who fail to comply with an order of the expert committee to remedy a violation, including orders to remedy, stop, suspend or seize related processing activities.

Non-Serious Offences

The expert committee may issue orders to remedy, stop, suspend or seize related processing activities, or may take other actions to stop/minimise damage within a specified period.

1.9 Enforcement Trends

Significant Enforcement Actions and Trends

January 2024 to January 2026

From "awareness-building" to real fines and public case summaries

Thailand's PDPC has moved into visible enforcement through administrative fines. This includes a landmark fine of THB7 million (the first high-profile fine under the PDPA) linked to a customer data leak that was later exploited in call centre scams. The findings included insufficient security measures and a failure to appoint a DPO.

Multi-case enforcement across sectors, including healthcare and processors

On 1 August 2025, the PDPC publicly highlighted five cases spanning both the public and private sectors (state agency online services, a private hospital's mishandling of medical record destruction, consumer businesses, and a reservation-system incident). Total fines to date amount to approximately THB21.5 million. Importantly, enforcement also extended to data processors (not only controllers), and repeatedly targeted deficiencies in security controls, breach reporting and DPO appointment as core failures.

Proactive investigations triggered by “signals” (dark web + social media), not just formal complaints

In January 2025, PDPC action in relation to an alleged breach followed a post advertising data for sale on the dark web, with the organisation instructed to investigate and report within 72 hours; the PDPC also described the role of its Eagle Eye unit in monitoring online sources (including the dark web and social platforms).

Regulator communications and reputational pressure via public channels

In April 2025, the PDPC publicly confirmed an investigation into a major company’s incident and indicated that it would require a detailed internal report (covering scope, root cause, impacts and risk assessment). The report was announced via PDPC’s Facebook page, signalling that enforcement risk can quickly become a public-facing issue.

Biometric data enforcement: suspension and deletion orders (Worldcoin/iris scanning)

On 24 November 2025, Thai authorities stated that the PDPC ordered relevant service providers/entities to suspend iris scanning and delete/destroy iris and personal data already collected. This action reflected heightened expectations for biometric processing (consent quality, necessity and security).

Practical Takeaways for Organisations

The last 24 months show that the PDPC is prioritising the following aspects (in practice).

- Security controls as the first line requirement (access controls, password practices, monitoring, periodic reviews/risk assessments).
- Breach response maturity being treated as equally important as prevention – prompt triage, documented risk assessment, timely notification and remediation.
- DPO and governance not treated as mere “paperwork” – absence or ineffectiveness treated as a serious aggravating factor.
- Processor governance as an enforceable obligation: due diligence, clear DPAs, oversight and ensuring processors can detect/notify/contain incidents.

- Healthcare/records handling and destruction as high-sensitivity areas – physical records and vendors remaining in scope.
- Proactive scrutiny if a leak becomes visible on the dark web or social media – the PDPC demands rapid clarification and evidence.
- Biometrics (eg, iris scans) attracting a heightened enforcement posture, including suspension and deletion orders.

In addition to enforcement under the PDPA, Thailand strengthened criminal enforcement through the Emergency Decree on Measures for the Prevention and Suppression of Technology Crimes (No 2) B.E. 2568 (2025) (effective from 13 April 2025). This decree introduces specific criminal offences targeting the misuse of personal data (including data relating to deceased persons) in connection with technology crimes. Where a person collects, possesses or discloses such data with intent to enable criminal activity, the penalty is imprisonment for up to one year and/or a fine of up to THB100,000. Where the conduct involves a commercial/exploitative element (eg, buying, selling, exchanging or unlawfully profiting from the data), the penalty increases to imprisonment for up to five years and/or a fine of up to THB500,000.

2. Privacy Litigation

2.1 Privacy Litigation Overview

As described in **1.8 Enforcement Proceedings and Fines**, the PDPA grants the expert committee enforcement powers to issue administrative orders to address any misconduct under the PDPA. However, most cases have been discharged or have ceased at the expert committee stage, and there are no publicly available high court cases in Thailand regarding personal data.

In addition to the powers of the expert committee, the PDPA provides for three types of liability:

- criminal liability;
- administrative liability; and
- civil liability.

For criminal liability, the authority may pursue criminal proceedings against any commercial operator that

has breached the PDPA. Any use or disclosure of sensitive data without consent that causes damage to the data subject is punishable by imprisonment of up to six months or a fine of up to THB500,000, or both. However, where any use or disclosure is carried out for the undue benefit of the commercial operator, the above-stated maximum term of imprisonment and the maximum fine will be doubled. In this regard, a director or manager of a juristic person may be subject to the same penalties as the juristic person.

As described in **1.8 Enforcement Proceedings and Fines**, there is a PDPC Notification on Administrative Penalties that governs the enforcement and criteria relating to administrative liabilities.

For civil liabilities, a damaged data subject may bring a civil suit against the controller and/or processor that has caused the damage. The PDPA expressly allows courts to award punitive damages, which are generally rare in Thailand, provided that such damages do not exceed twice the amount of actual damages (if the court considers the breach to be severe). As this civil liability is based on tort law and privacy cases often involve more than one impacted data subject, class actions are allowed for privacy cases.

2.2 Recent Case Law

As described in **1.8 Enforcement Proceedings and Fines** and **2.1 Privacy Litigation Overview**, there have been no significant litigation cases in the area of privacy or data protection law in Thailand, as most matters are typically resolved at the expert committee level. At present, there is only a first-instance court judgment concerning the unlawful sale of personal data, and it remains to be seen whether this approach will be upheld or further clarified by the higher courts.

2.3 Collective Redress Mechanisms

In Thailand, the concept of collective redress exists within the legal framework, commonly referred to as a “Class Action”. However, its application and procedural development remain limited and continue to evolve. Victims of data protection violations are entitled to file a case against offenders through the Class Action mechanism, as data protection breaches typically fall within the scope of tort claims. In practice, in high-profile cases (affecting many individuals), the

Office of the PDPC often encourages all victims to provide their information before an investigation is initiated and appropriate action is taken.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Thailand does not currently have a single, horizontal “non-personal data act” that comprehensively governs ownership/access/use-sharing of machine-generated or industrial data (eg, IoT device data) in the same manner as the EU Data Act. Instead, non-personal data is mainly governed through a patchwork of:

- cybersecurity and cybercrime laws (security/incident response and criminal offences);
- trade secret/IP rules (confidentiality and proprietary datasets); and
- public sector data governance and access frameworks (digital government, open data, official information).

3.2 Interaction of Data Regulation and Data Protection

The PDPA applies as a supplementary law to other applicable statutes, to the extent that it does not conflict with such laws.

3.3 Rights and Obligations Under Applicable Data Regulation

There is no specific law addressing the rights and obligations, as mentioned in **3.1 Objectives and Scope of Data Regulation**.

3.4 Regulators and Enforcement

There is no specific law addressing regulators and enforcement matters, as mentioned in **3.1 Objectives and Scope of Data Regulation**.

4. Sectoral Topics

4.1 Use of Cookies

Currently, there is no specific legislation in Thailand that regulates the use of cookies. However, as the use of cookies is considered the processing of personal

data, it falls under the principles of the PDPA, which apply to different types of cookies as follows.

- Strictly necessary cookies or essential cookies are necessary for the basic functioning of a website. Explicit consent is not required as they can be used on a contractual basis.
- Performance and functional cookies are used to enhance user experience and improve website performance. Explicit consent from users is required prior to the use of such cookies.
- Targeting and advertising cookies track user behaviour for personalised advertising and are not necessary for any functions on the website, so explicit consent is required.

For the general requirements applicable to any types of cookies, the PDPA requires controllers to provide clear information about the purpose and function of each type of cookie, typically through a cookie policy and cookie banners or pop-ups that inform users and obtain their consent. The information provided shall be consistent with other notifications for data processing provided to data subjects – the types of cookies used on the website, the personal data to be processed, the purposes of processing, the retention period, the rights of data subjects, etc. In addition, users must be given the ability to manage their cookie preferences, withdraw consent, and access or delete data collected through cookies.

4.2 Personalised Advertising and Other Online Marketing Practices

Generally, online marketing may be based on the legitimate interests of the data subject, or on the consent given thereby. Personalised advertising is regarded as overly intrusive for data subjects, and therefore consent under the PDPA is required.

In addition to the PDPA, online marketing activities may fall within the scope of computer data or electronic mail under the Computer-Related Crime Act B.E. 2550 (2007). Where an operator sends any computer data or electronic data (such as email, SMS or comments) to another person in a manner that disturbs that person, such operator must provide that person with an easy means to cancel or notify the wish to refuse receipt of such computer data or electronic

mail (ie, an opt-out option). Failing to do so may result in a fine not exceeding THB2 million. Once any person has requested to refuse such receipt, the operator must stop sending such marketing messages immediately (ie, no later than seven days after the request).

4.3 Employment Privacy Law

Similar to other relationships, the enactment of the PDPA has significantly impacted the employment relationship, particularly in relation to how employers collect, use and manage employees' personal data. The PDPA requires employers to obtain specific consent from employees before collecting personal data or sensitive personal data, while ensuring transparency from recruitment throughout the entire employment lifecycle.

The PDPA emphasises data minimisation and purpose limitation, requiring employers to collect only the personal data necessary for specific purposes related to employment – completing the employment process, providing employee benefits, managing payroll, etc. Employers must ensure that personal data is used solely for the purposes for which it was collected and in accordance with the information provided in the employees' privacy policy. In addition, employers are required to maintain data security measures and comply with other provisions regarding the controllers' obligations under the PDPA (please see 3.1 **Objectives and Scope of Data Regulation** for more detail).

As data subjects, employees are granted several rights under the PDPA, such as:

- the right to access, correct and delete their personal data;
- the right to withdraw consent for data processing; and
- other related rights.

Employers must establish procedures to facilitate these rights, allowing employees to exercise control over their personal data and thereby enhancing privacy and trust in the employer-employee relationship.

4.4 Data Protection in M&A

There are no specific regulations in Thailand concerning the transfer of personal data in asset deals. Only

the general PDPA provisions are applicable to this area.

5. International Considerations

5.1 Restrictions on International Data Transfers

The PDPA does not provide for the concept of absolute restriction for any type of transfer of personal data outside the jurisdiction of Thailand. Instead, controllers, as transferors, may be subject to several obligations and/or must ensure that the transferee meets the qualifications prescribed under the PDPA.

In general, in the case of transferring personal data outside Thailand, the countries in which the transferee is located should have adequate personal data protection measures in place. The list of countries deemed to have adequate personal data protection measures is set to be prescribed by the PDPC; however, such list has not yet been issued. Two key criteria for assessing whether a country is deemed to have adequate personal data protection measures are:

- whether the legal safeguards for personal data protection in such country are of a standard equivalent to or higher than those under the PDPA; and
- whether such country has a competent authority or organisation responsible for enforcing the above-mentioned safeguards.

In any event, even after such list is prescribed, several exemptions exist under which a controller may transfer personal data to countries outside such list (transfers necessary for compliance with the law, transfers based on the data subject's consent, transfers required for the performance of a contract to which the data subject is a party, etc).

Another exemption to the limitation on personal data transfers to only those countries included in such list applies where the following conditions are fulfilled:

- such transfer is made within a group of undertakings or enterprises; and

- such transferor of the personal data applies binding corporate rules (BCRs) that have already been approved by the PDPC office to such transfer.

Where no list is prescribed for those countries deemed to have adequate personal data protection measures, or where the BCRs have not yet been approved by the PDPC office, the PDPA stipulates that the transferor must provide appropriate security measures in accordance with the rights of the data subjects, together with effective legal remedial measures, such as appropriate standard contractual clauses (SCCs) for cross-border transfers and certification mechanisms. Under a PDPA notification, SCCs based on the ASEAN Model Contractual Clauses for Cross-Border Data Flows and GDPR SCCs are acceptable.

5.2 Government Notifications and Approvals

Cross-border transfers do not require any government notification or approval.

5.3 Data Localisation Requirements

In certain cases, operators have to retain some documents on their premises, such as accounting documents and VAT certificates. However, operators can duplicate and transfer such data outside Thailand (see 5.1 Restrictions on International Data Transfers for more details).

5.4 Blocking Statutes

There are no blocking statutes under Thai privacy laws.

5.5 Recent Developments

On 29 September 2025, the PDPC issued the Rules on the submission, consideration, examination, certification and supervision of personal data protection policies within the same affiliated business or group of undertakings (B.E. 2568 (2025)), which establish a formal certification regime for BCRs under the PDPA. The Rules confirm that there are two types of BCRs: BCRs for Controllers (BCR-C) and BCRs for Processors (BCR-P), each of which may be used as an appropriate safeguard for cross-border personal data transfers from Thailand regardless of the adequacy status of the destination country. A Thai “anchor” entity must be established under Thai law and maintain a place of business in Thailand (eg, the Thai headquarters or

Contributed by: Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsatapom,
Chandler Mori Hamada Limited

another designated Thai group member responsible for PDPA matters) and act as the Liable BCR Member for the purposes of PDPC interaction and enforcement.

Applications and supporting documents must be prepared in Thai (with certified translations where necessary) and submitted to the PDPC Office. The PDPC Office conducts a completeness check within 15 days and aims to complete substantive review within approximately 180 days. Possible outcomes of the review are approval, conditional approval (subject to corrections) or rejection, and conditional decisions or rejections may be appealed. BCR certification remains valid indefinitely unless amended or revoked by the PDPC, and no official government filing fee is currently imposed under the Rules. This formal regime provides a durable, programmatic compliance framework for cross-border transfers among affiliated entities, potentially reducing reliance on multiple bilateral mechanisms such as SCCs.

The introduction of this certification process signals the PDPC's move towards a more clearly defined and structured pathway for intra-group transfers under the PDPA.

Trends and Developments

Contributed by:

Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn
Chandler Mori Hamada Limited

Chandler Mori Hamada Limited combines an international standard of practising law with decades of local experience in the Thai legal environment. The team of more than 100 lawyers in Thailand is internationally recognised for its legal expertise in anti-trust and competition, aviation, banking and project financing, capital markets, corporate and M&A, data

privacy and data protection, dispute resolution, energy, natural resources and infrastructure, insurance, labour and employment, real estate, REITs, regulatory and public policy employment and tax, restructuring and insolvency and technology, and media and telecommunications.

Authors



Jutharat Anuktanakul is a partner at Chandler Mori Hamada. She has represented Thai and international clients in preparing applications for investment promotion to the Board of Investment and the Industrial Estate

Authority of Thailand in a wide variety of sectors, including energy, telecommunications, electronics and software. As a specialist in corporate law, she has represented numerous clients in share or asset acquisitions, partial and complete business transfer transactions, and registration of regional, branch and representative offices of foreign corporations. Jutharat also advises on other regulatory and data protection compliance strategies.



Pitchaya Roongroajsataporn is an associate at Chandler Mori Hamada and a member of the corporate and mergers & acquisitions practice group. She has a particular focus on the technology, media and

telecommunications (TMT) sector, including data protection. Her experience includes advising on a broad range of data protection issues, including the PDPA in Thailand, applying for digital asset business licences and providing regulatory advice related to the technology sector.



Suphakorn Chueabunchai is a senior associate at Chandler Mori Hamada. He specialises in corporate and regulatory matters, with experience in advising on mergers and acquisitions and due diligence of Thai target

companies. He also has significant experience in privacy and data protection law, advising leading clients on PDPA compliance and conducting gap analyses across the financial services, modern trade, automotive and pharmaceutical sectors. In addition, Suphakorn advises digital platforms and e-commerce businesses on regulatory compliance, including licensing requirements and applicable laws.

Contributed by: Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsatapom,
Chandler Mori Hamada Limited

Chandler Mori Hamada Limited

31st and 36th Floors
Sathorn Square Office Tower
98 North Sathorn Road
Silom
Bangrak
Bangkok 10500
Thailand

Tel: +662 009 5000
Fax: +662 009 5080
Email: business-development@morihamada.com
Web: chandler.morihamada.com

CHANDLER MORI HAMADA

Thailand's Personal Data Protection Act B.E. 2562 (2019) (PDPA) has moved decisively from a "compliance-building" phase into a more enforcement-oriented phase. Although enacted in 2019, the PDPA only became fully effective in 2022, placing 2025 at a critical inflection point: long enough for organisations to have built baseline compliance frameworks, yet recent enough that regulatory expectations are still being shaped through early precedent, subordinate legislation and case-based enforcement.

Against this backdrop, 2025 stands out as a year of visible regulatory momentum, characterised by:

- a meaningful expansion in administrative enforcement, including multiple fines across the public and private sectors;
- a sharper focus on breach preparedness and vendor governance;
- a more proactive monitoring posture, including the continued operationalisation of PDPC Eagle Eye and attention to high-risk processing activities such as biometric data; and
- sustained development of the PDPA "ecosystem", especially reform discussions, voluntary certification ("Trust Mark") and cross-border transfer mechanisms such as Binding Corporate Rules (BCRs).

This article highlights four core developments from 2025 that will shape the trends and developments landscape in 2026:

- the Personal Data Protection Committee's (PDPC) five-case wave of administrative penalties;
- proactive enforcement via PDPC Eagle Eye, including the widely reported "iris scan in exchange for crypto tokens" case involving World/Worldcoin;
- the public consultation process on potential amendments to the PDPA; and
- the maturation of compliance infrastructure, most notably preparations for Trust Mark and the formalisation of the BCR certification framework.

Enforcement in 2025: From Warning Signals to Repeatable Precedent

Eight administrative fines across five cases (public and private sectors)

On 1 August 2025, Thailand's PDPC publicly announced the imposition of eight administrative fines across five non-compliance cases involving both public and private entities. The announcement was notable not only for the aggregate value involved (reported at approximately THB21.5 million to date), but also for the diversity of fact patterns, ranging from cyberattacks affecting online public services to operational failures in document destruction and vendor-managed reservation systems.

A key signal from this enforcement wave is the PDPC's willingness to treat the PDPA as an operational governance framework, encompassing security controls, vendor oversight and incident response, rather than merely as a documentation exercise focused on privacy notices and consent forms. In several cases, the

Contributed by: Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn,
Chandler Mori Hamada Limited

PDPC imposed penalties on both the data controller and a data processor involved in the processing activities, reinforcing that accountability under the PDPA is not confined to the most visible brand name in the processing chain.

What the five cases indicate regulators care about most

As reflected in public reporting, the five cases from 2025 provide a practical “compliance map” of regulatory priorities.

Case 1 – state agency online services (cyber-attack and dark web leakage)

A cyber-attack against a state agency’s web application reportedly resulted in the leakage of personal data relating to approximately 200,000 data subjects. The PDPC’s findings pointed to fundamental security deficiencies, including weak password controls, the absence of a formal risk assessment, and a failure to conduct regular reviews and update security measures. The regulator also identified a governance lapse – namely, the absence of a data processing agreement with the software developer acting as a data processor. As a result, the PDPC imposed administrative fines of THB153,120 on both the state agency and the developer.

Although the monetary penalties imposed on the public sector entity were relatively modest compared with those more commonly imposed on private sector organisations, this case is significant in underscoring the PDPC’s position that state agencies are subject to the PDPA and its enforcement regime on an equal footing. Importantly, the decision also clarifies that being the victim of a cyber-attack does not, in itself, amount to wrongdoing. However, where an organisation fails to implement appropriate and proportionate security and governance measures, it may still be held accountable as a wrongdoer under the PDPA, notwithstanding the involvement of third-party attackers.

Case 2 – private hospital (outsourced document destruction failure)

A private hospital engaged an individual contractor to destroy patient medical record documents. The contractor reportedly mishandled the documents and reused them as wrapping for sweets, resulting

in the leakage of personal and medical data of more than 1,000 individuals and subsequent public exposure via social media. Beyond the inherently sensitive nature of health data, the PDPC focused on the hospital’s failure to implement adequate security and oversight measures, as well as its failure to report the breach in accordance with the PDPA. The hospital was fined THB1,210,000, while the contractor was fined THB16,940.

This case is notable not only for turning what was once regarded as an anecdotal “joke” about the reuse of paper for food packaging in Thailand into a concrete compliance failure, but also for illustrating the PDPC’s proportional approach to penalties. The significant disparity between the fines imposed on the hospital and on the individual contractor demonstrates that the regulator takes into account the nature, scale and capacity of the offender, as well as the degree of organisational responsibility and control, when determining administrative sanctions.

Case 3 – “computer and accessories trading giant” (breach linked to call centre scams)

More than 100 data subjects reportedly complained following call centre scams tied to a breach incident. The PDPC cited a lack of security measures, failure to report breach incidents, and failure to appoint a DPO. The company was fined THB7 million (with public reporting indicating that the company’s revenue and size were taken into account).

This case closely mirrors the landmark enforcement action taken by the PDPC in 2024, in terms of both the factual circumstances and the legal bases for liability. Taken together, these cases suggest that the PDPC is developing a consistent enforcement benchmark for large-scale data breaches involving inadequate security governance, delayed breach notification and the absence of a DPO.

Case 4 – cosmetics company

A cosmetics company reportedly suffered leakage of personal data to a call centre gang due to inadequate security measures, and also failed to notify the PDPC of the breach incident. The company was fined THB2,500,000.

Contributed by: Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn,
Chandler Mori Hamada Limited

Case 5 – collectible toy company + processor (reservation system compromise)

A collectible toy company used a data processor for a reservation system, which was compromised for a brief period (reported to be around ten minutes), resulting in unauthorised amendments to approximately 200,000 records. The PDPC fined both parties: the toy retailer THB500,000 and the data processor THB3 million, highlighting that processors can face serious exposure where they fail to contain incidents, notify controllers or support remediation.

Practical enforcement themes emerging from the cases

Across these fact patterns, three recurring compliance failures stand out, each of which is likely to remain front and centre in 2026.

Security measures and security governance

The PDPC repeatedly focused on whether security measures were “appropriate” and subject to ongoing review, including risk assessments, access controls, and privacy and security by design. It also examined whether data retention, deletion and destruction practices were appropriate and ensured that personal data was not retained longer than necessary.

Breach reporting discipline and incident response maturity

Several penalties emphasised failures to notify the regulator (and in some cases, failures to notify counterparties within controller–processor relationships), demonstrating that “late or missing reporting” is no longer regarded as a minor technicality.

DPO designation and vendor governance (including DPAs)

In addition to substantive security controls, the PDPC’s enforcement posture continues to treat governance obligations – ie, the designation of a DPO where required and the implementation of contractual controls via DPAs – as “core compliance” requirements rather than optional best practice.

In short, enforcement actions in 2025 convert PDPA compliance into an enterprise risk-management issue that must sit with senior management, IT/security and

procurement/vendor owners – not only legal/compliance teams.

Proactive Monitoring and High-Risk Processing: PDPC Eagle Eye and the World/Worldcoin Biometrics Case

PDPC Eagle Eye as an operational enforcement capability

A further indicator of intensifying enforcement is the regulator’s investment in proactive monitoring functions. Over the past year, PDPC Eagle Eye has operated as a dedicated unit using technology to monitor and detect personal data leaks, including scanning search engines, online sources and dark web locations, as well as co-ordinating with relevant agencies on follow-up actions. In many instances where there is public reporting of personal data breaches or improper use of personal data, PDPC Eagle Eye has published preliminary details through its online channels to raise public awareness of personal data protection threats. This has, at times, led organisations to perceive such disclosures as reputationally damaging, even where the underlying facts have not yet been fully verified.

This development is significant for organisations because it fundamentally alters the practical risk equation: regulatory enforcement no longer depends solely on a complaint from a data subject. Where a data leak is visible online, or otherwise detectable through proactive monitoring, organisations may be contacted by the regulator even in the absence of any formal complaint by affected individuals.

The “iris scan in exchange for crypto tokens” enforcement action (World/Worldcoin)

The most high-profile illustration of the PDPC’s 2025 posture is the enforcement action against the business offering iris scanning in exchange for cryptocurrency tokens, widely reported as World (formerly Worldcoin).

In late November 2025, multiple outlets reported that Thai authorities ordered the operator to halt the iris scan service and delete biometric data of approximately 1.2 million users in Thailand, citing PDPA breaches and concerns around unlawful consent and biometric data risk.

Contributed by: Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn,
Chandler Mori Hamada Limited

Key reported themes in the regulator's reasoning are directly relevant to compliance expectations for 2026, as follows.

- Biometric data is high-risk by default. Iris data is commonly treated as biometric data, which typically attracts heightened compliance scrutiny because it is difficult to change if compromised and can be used for identity verification.
- "Consent" must be truly voluntary – financial inducement creates risk. Reporting emphasised concerns that offering crypto tokens in exchange for consent may undermine voluntariness, making consent potentially invalid under PDPA principles.
- Purpose limitation and transparency remain core principles. Media coverage reflects regulatory concerns that actual data use may extend beyond the purposes communicated at the point of collection. Clear, specific and easily understandable consent language may help mitigate the risk of challenges from data subjects regarding the scope of use.

For 2026, the practical takeaway is that the PDPC is willing to take strong action where a processing model is built around high-risk data (biometrics) combined with incentives that may compromise "freely given" consent and create downstream transfer/security concerns. This is a clear warning for any business operating digital ID, fintech-onboarding, biometric access control or consumer-facing "reward for data" models.

PDPA Reform Discussions: Public Consultation on Proposed Amendments in 2025

2025 also saw a rise in momentum toward possible legislative reform of the PDPA. As the PDPA has now been in force for approximately five years, policymakers have begun reviewing whether certain provisions should be refined or adjusted in light of practical implementation and enforcement experience. Toward the end of 2025, a draft amendment bill relating to the PDPA was released for public consultation, although the process was not completed.

During the consultation process, stakeholders expressed both supporting and opposing views in relation to the proposals put forward by the drafting committee. This diversity of feedback suggests that

the content of any final amendments may differ from the draft, and reinforces the need to closely monitor the version that is ultimately promulgated.

Even without predicting the final form of any amendments, the consultation materials provide useful insight into the types of issues under consideration, including the following examples:

- repositioning the PDPA as the primary legal framework for personal data processing, rather than merely a baseline compliance standard, to ensure greater legal clarity and consistency across sectors;
- clarifying and refining the definitions of "data controller" and "data processor" to reduce interpretive uncertainty in complex processing and outsourcing arrangements;
- revisiting the list of sensitive personal data to better align it with Thailand's legal, social and cultural context; and
- improving the clarity of consent requirements, particularly to prevent practices where consent is effectively exchanged for goods, services or benefits in a manner that undermines its voluntariness.

These proposed areas of adjustment are illustrative only, and the scope and substance of any amendments may evolve as deliberations continue. Further changes may be introduced as part of the final outcome, and close attention will need to be paid to future guidance and decisions issued by the PDPC.

Looking ahead to 2026, this reform dialogue is relevant in two key respects.

- First, it signals that Thailand may be entering a "second-stage PDPA" phase: following initial implementation and early enforcement, attention is shifting toward refinement, clarification and the reduction of practical compliance friction for both private and public sector use cases.
- Second, the legislative review process is likely to interact with enforcement practice. As regulatory precedent develops, recurring ambiguities and operational challenges become more visible, creating a feedback loop between enforcement experience and legislative fine-tuning.

Contributed by: Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn,
Chandler Mori Hamada Limited

Building the Compliance Ecosystem: Trust Mark Preparations and BCR Certification Rules

Trust Mark: moving from compliance to demonstrable assurance

The PDPC has been developing compliance infrastructure that may influence market behaviour in 2026 – most notably through a proposed “data protection standard mark” or “Trust Mark”.

The PDPC is currently preparing the final draft of the Trust Mark questionnaire, with an announcement expected in the second or third quarter of 2026. This initiative reflects the regulator’s intention to establish a structured framework through which organisations may demonstrate alignment with PDPA requirements and recognised data protection practices.

From a trends perspective, the Trust Mark initiative is significant because it has the potential to reshape incentives beyond merely avoiding regulatory penalties. If the Trust Mark is used in procurement processes, public tenders, platform partnerships or consumer-facing trust signals, whether formally or informally, it may emerge as a meaningful commercial differentiator. Over time, this could shift PDPA compliance from a predominantly reactive legal risk management exercise towards a more proactive model focused on assurance and competitiveness, particularly for service providers handling large volumes of personal data, such as those in e-commerce, cloud and outsourcing services, digital health, fintech and data analytics

BCR certification: cross-border transfer compliance becomes operational

Cross-border transfer compliance has been one of the most challenging operational areas under the PDPA, especially for multinational groups that routinely share data within affiliated entities.

A major 2025 development was the issuance of formal rules for the review and certification of BCRs. The PDPC Office published its Regulations on the Review and Certification of BCRs (B.E. 2568 (2025)) on 29 September 2025, establishing clearer pathways for intra-group transfers under Section 29 of the PDPA.

Even more importantly, the PDPC Office approved BCRs for two companies operating in Thailand on 30 September 2025, marking an important “first concrete progress” milestone in moving BCRs from theory into practice.

Key features of the 2025 BCR framework that will shape trends in 2026 include:

- two categories of BCRs: BCRs for Controllers (BCR-C) and for Processors (BCR-P);
- Thai-language documentation requirements, including expectations around translation formalities;
- a published review timeline (up to 180 days from submission of complete documentation) and no government fee stated for certification; and
- no fixed expiry date, although BCRs remain subject to amendment/suspension/revocation and ongoing compliance expectations.

For multinational groups, the 2025 BCR rules (together with the first approvals) meaningfully shift BCRs into the category of “realistic strategic options” for transfer compliance, particularly where groups are seeking a durable intra-group mechanism rather than transaction-by-transaction contracting.

For 2026, it is reasonable to expect more organisations to explore BCR certification, especially those already operating under EU/UK GDPR BCR regimes and seeking to align their global privacy governance models with Thai PDPA requirements.

Practical Checklist for Organisations Operating in Thailand in 2026

In light of developments in 2025, the following actions are likely to represent the most defensible “baseline priorities” entering 2026.

Breach readiness as a tested capability

Breach simulations must be run, and it must be ensured that incident response processes can triage PDPA notification triggers, co-ordinate with processors, and produce regulator-ready reporting.

Contributed by: Jutharat Anuktanakul, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn,
Chandler Mori Hamada Limited

Implementation of appropriate security measures (beyond documentation)

Preparing documentation alone (such as privacy policies or consent forms) is not sufficient to fulfil PDPA obligations. Organisations must implement appropriate security measures proportionate to their specific risks, including technical, organisational and administrative safeguards. This has become increasingly critical in light of more active and substantive enforcement by the Thai regulator.

Vendor governance and DPAs as operational controls

Processor arrangements must be audited (particularly with IT vendors, cloud/hosting providers, outsourced call centres and destruction service providers), confirming:

- contractual coverage;
- security requirements;
- notification obligations; and
- audit/monitoring rights.

DPO decision-making and evidence trail

Where DPO designation is required (or where the position is borderline), the assessment must be documented, and it must be ensured that the DPO function has visibility and authority.

High-risk processing governance (biometrics, health, identity)

Biometric projects must be treated as initiatives subject to “special scrutiny”, with explicit consent design, voluntariness assessment, DPIA-style risk assessment, retention/deletion logic and transfer controls.

Cross-border transfer roadmap

Where group operations rely on intra-group transfers, it must be assessed whether BCR certification is feasible and valuable under the new PDPC’s framework, especially where GDPR BCRs are already in place.



Law and Practice

Contributed by:

Bora Yazıcıoğlu, Yağız Soymen, İbrahim Yıldırım and Ezgi Girenay
YAZICIOGLU Legal

Contents

1. Legal and Regulatory Framework p.512

- 1.1 Overview of Data and Privacy-Related Laws p.512
- 1.2 Rights and Obligations p.513
- 1.3 Special Categories of Personal Data p.514
- 1.4 Processing of Personal Data for Research and Development Purposes p.514
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.515
- 1.6 Data Breach Requirement p.515
- 1.7 Regulators p.516
- 1.8 Enforcement Proceedings and Fines p.516
- 1.9 Enforcement Trends p.518

2. Privacy Litigation p.518

- 2.1 Privacy Litigation Overview p.518
- 2.2 Recent Case Law p.519
- 2.3 Collective Redress Mechanisms p.519

3. Requirements for the Protection and Processing of Non-Personal Data p.519

- 3.1 Objectives and Scope of Data Regulation p.519
- 3.2 Interaction of Data Regulation and Data Protection p.519
- 3.3 Rights and Obligations Under Applicable Data Regulation p.520
- 3.4 Regulators and Enforcement p.520

4. Sectoral Topics p.520

- 4.1 Use of Cookies p.520
- 4.2 Personalised Advertising and Other Online Marketing Practices p.521
- 4.3 Employment Privacy Law p.521
- 4.4 Data Protection in M&A p.523

5. International Considerations p.523

- 5.1 Restrictions on International Data Transfers p.523
- 5.2 Government Notifications and Approvals p.525
- 5.3 Data Localisation Requirements p.525
- 5.4 Blocking Statutes p.526
- 5.5 Recent Developments p.526

YAZICIOGLU Legal is an Istanbul-based boutique technology law firm. The firm focuses on legal matters related to technology, media & telecommunications and data protection/cybersecurity. It also has solid expertise in cross-border transactions, corporate and commercial matters, intellectual property, regulatory compliance, e-commerce, consumer protection, and dispute resolution. YAZICIOGLU Legal has a dedicated team of 16 lawyers working on data protection and cybersecurity. The majority of the firm's workload

involves data protection-related matters. In particular, the firm is known for successfully representing its clients on investigations and data breaches before the Turkish Data Protection Authority. It also provides assistance to several clients, both local and international, including but not limited to Acer, Reddit, and Workday in ensuring compliance with data protection legislation, particularly in cross-border data transfers. The firm is also a Bronze Corporate Member of the International Association of Privacy Professionals (IAPP).

Authors



Bora Yazıcıoğlu is the managing partner at YAZICIOGLU Legal. He has significant experience in advising national and international clients on various aspects of data protection, cybersecurity, and e-commerce law.

Bora has represented several major clients on data breaches and investigations before the Turkish Data Protection Authority. He is one of the founding members and the current president of the Data Protection Association of Türkiye. Bora acts as the data controller representative for Zoom, Acer, Cerus, and Ookla in Türkiye.



Yağız Soymen is a senior associate at YAZICIOGLU Legal. He has experience in providing consultancy, audit, and training services regarding compliance processes with data protection regulations. He also works

as lead auditor for ISO/IEC 27001 and ISO/IEC 27701. Since 2021, he has been serving as co-director of the Privacy Innovation Lab at Istanbul Bilgi University, where he contributes to training and research activities in the field of data privacy.



İbrahim Yıldırım is a mid-level associate at Yazıcıoğlu Legal. He focuses mainly on various fields of law, including personal data protection, AI, IT law, e-commerce law, contract law, international arbitration, and labour law.



Ezgi Girenay is a legal trainee at YAZICIOGLU Legal. She is working in the fields of data protection, cybersecurity, and e-commerce law.

YAZICIOGLU Legal

NidaKule – Göztepe
Merdivenköy Mahallesi Bora Sokak
No: 1 Kat: 7 34732
Kadıköy / İstanbul
Türkiye

Tel: +90 216 468 88 50
Fax: +90 216 468 88 01
Email: info@yazicioglulegal.com
Web: www.yazicioglulegal.com

YAZICIOGLU
— LEGAL —

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Right to Protection of Personal Data

The right to protection of personal data is regulated under the Constitution of the Republic of Türkiye (the “Constitution”) as an individual right.

According to Article 20 (3) of the Constitution, the right to protection of personal data includes the right to:

- be informed about the processing of personal data;
- have access to personal data;
- rectification or deletion of personal data; and
- be informed about whether personal data is used in accordance with the appropriate purposes.

According to the same Article, personal data may be processed if the processing is allowed by the law, or if the data subject gives explicit consent. The Article finally states that the procedures and principles of processing personal data must be regulated by law.

The Turkish Data Protection Law

Pursuant to the Constitution, the Turkish Data Protection Law (DP Law) was enacted, which is the first general law that regulates the rules for processing personal data in Türkiye. It entered into force on 7 April 2016.

Although it came into force only one month before the European Union General Data Protection Regulation (GDPR), the DP Law was drafted considering only EU Directive 95/46/EC. Currently, efforts are underway to align the DP Law with the GDPR. As part of these efforts, the Law on Amendments to the Criminal Procedure Law and Certain Laws, which also includes amendments to the DP Law (DP Law Amendments) was published on 12 March 2024.

Upon the entry into force of the DP Law Amendments on 1 June 2024, these efforts were followed by the publication of the By-law on the Procedures and Principles Regarding the Transfer of Personal Data Abroad (By-law on Data Transfers Abroad) and the Guidelines on the Transfer of Personal Data Abroad (Guidelines on Transfers Abroad), refer to the European Data Pro-

tection Board’s (EDPB) guidelines in interpreting the new cross-border transfer rules.

The DP Law does not expressly regulate its territorial scope. Nevertheless, the Turkish Data Protection Authority (DPA) has consistently taken the position that the DP Law may apply to data controllers established outside Türkiye where certain criteria are met. Although these criteria are not explicitly set out in the legislation, they can be inferred from the DPA’s decisions. In certain decisions, the DPA adopts an effects-based approach, pursuant to which the DP Law is applicable where processing activities are carried out or produce effects in Türkiye. In other instances, the DPA has also applied a targeting-based approach, where the DP Law applies when individuals in Türkiye are targeted through the provision of services or profiling activities.

The DP Law establishes a framework by outlining the general obligations and principles for data processing activities. Its implementation is further supported by secondary legislation, resolutions and guidelines issued by the DPA, including:

- the By-law on the Deletion, Destruction, or Anonymisation of Personal Data (By-law on the Disposal of Personal Data);
- the By-law on the Registry of Controllers;
- the By-law on Data Transfers Abroad;
- the Communique on Principles and Procedures to Be Followed in Fulfilment of the Obligation to Inform (Communique on Obligation to Inform); and
- the Communique on Principles and Procedures for the Request to Controllers.

Turkish Cybersecurity Law

The Turkish Cybersecurity Law (Cybersecurity Law) entered into force on 19 March 2025. Cybersecurity Law introduces a comprehensive legal framework governing cybersecurity in Türkiye and aims to establish a centralised regulatory structure in a field that was regulated through dispersed legal instruments and sector-specific rules.

Before the Cybersecurity Law, cybersecurity obligations were addressed through various instruments which primarily applied to public institutions and criti-

cal infrastructure operators. In addition, the DP Law imposed obligations regarding the security of personal data, and certain sector-specific regulations also contained cybersecurity provisions. However, these rules did not establish a comprehensive cybersecurity regime. The Cybersecurity Law therefore functions as an overarching framework, and secondary legislation is expected to regulate its implementation further.

The Cybersecurity Law broadly applies to public institutions, private entities, real persons, and other organisations operating in cyberspace. It grants the Cybersecurity Presidency extensive supervisory powers and imposes several obligations on organisations, including co-operation with audits, implementation of cybersecurity measures, and notification of cybersecurity incidents, with administrative fines and criminal sanctions introduced for non-compliance.

Turkish Criminal Law

Certain actions that violate the protection of personal data are defined as crimes in the Turkish Criminal Law (“TCrC”). The TCrC also outlines criminal sanctions for these violations:

- unlawful recording of personal data is subject to imprisonment of one to three years;
- unlawful transfer, publication, or acquisition of personal data is subject to imprisonment of two to four years – if these are realised by exploiting the advantages of a profession or art, such actions are subject to imprisonment of three to six years; and
- failure to destroy personal data after the retention period set forth in the law has passed is subject to imprisonment of two years.

The investigation may commence without requiring a complaint. There is no established jurisprudence on how criminal sanctions will be harmonised with the DP Law.

Turkish Civil Law and the Turkish Code of Obligations

Personal data is considered a part of personality under Turkish law; as such, it is also protected under the protection of personality rights in the Turkish Civil Law (TCiC). Therefore, an individual whose right to

the protection of personal data is violated may file a lawsuit before civil courts.

General provisions of the Turkish Code of Obligation (TCO) may also apply in cases of breach of an obligation, particularly when it comes to liability for damages and compensation for harm caused by violating contractual or non-contractual obligations.

Per the TCiC and the TCO, data subjects can not only seek compensation but also ask courts to:

- prevent a threatened infringement;
- cease an existing infringement; and/or
- make a declaration that the infringement is unlawful.

Other

There are also sector-specific regulations governing the processing of personal data in areas such as telecommunications, banking, electronic payment, health, and education.

It is important to consider these legislations, as the DP Law specifies that provisions in other laws regarding the deletion, destruction, or anonymisation, or transfer of personal data, are reserved.

1.2 Rights and Obligations

General Principles and Data Subject Rights

Personal data processing is governed by the principles of lawfulness, fairness, accuracy, and being up to date. Processing must be for specific, explicit, and legitimate purposes, remaining relevant, limited, and proportionate to the intended use. Under the DP Law, data subjects have the right to learn whether their personal data is processed, obtain information about any such processing, its purposes, and the third parties to whom the data is transferred, to request the rectification or deletion of their personal data and the notification of such actions to third parties, to object to decisions based solely on automated processing, and to claim compensation for damages arising from unlawful processing.

Obligations established by the DP Law are imposed on controllers, who determine the purpose and means of processing personal data. Key obligations include;

- Registration to the Registry of Controllers (VERBIS): Controllers meeting specific criteria must register with the VERBIS. Those obliged controllers must also maintain a data processing inventory and implement a Personal Data Retention and Destruction Policy. Additionally, they must designate a “contact person” responsible for submitting information to VERBIS and facilitating communication with the DPA.
- Privacy Notices: Controllers must provide data subjects with clear notices detailing the processing activity.
- Technical and Administrative Measures: Controllers must implement appropriate organisational and technical safeguards to prevent unauthorised access and unlawful processing.
- Request Management: Controllers must respond to data subject requests within 30 days.
- Breach Notification: Any personal data breach must be notified to the DPA without any delay and within 72 hours of becoming aware of the breach, where possible. Affected individuals must also be informed promptly.
- Processor Oversight: Controllers are jointly responsible for ensuring that processors implement the necessary technical and administrative measures while processing data on their behalf.

1.3 Special Categories of Personal Data

Special categories of personal data are defined in DP Law as follows: data relating to race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership of associations, foundations or trade unions, data concerning health, sexual life, criminal convictions and security measures, and biometric and genetic data.

The processing of special categories of personal data is governed by Article 6 of the DP Law and secondary regulations issued by the DPA.

The processing conditions specified in Article 6 of DP Law are as follows:

- explicit consent;
- being explicitly prescribed by law;

- being mandatory to protect the life or physical integrity of a person who is physically unable to give consent;
- being made public by the data subject;
- being mandatory for the establishment, exercise, or protection of a right;
- being mandatory for the fulfilment of legal obligations in the fields of employment, occupational health and safety, social security, or social assistance;
- being mandatory for activities carried out by foundations, associations, or other non-profit organisations for their members, provided the data is not disclosed to third parties; and
- being mandatory for medical diagnosis, treatment, care services, or the planning and management of health services and financing.

Controllers must also comply with the DPA's decision, setting out specific technical and administrative measures for the processing of special categories of personal data.

DP Law does not foresee a specific regime for the processing of minors' personal data; however, the DPA occasionally publishes guidelines and materials aimed at raising awareness.

1.4 Processing of Personal Data for Research and Development Purposes

Unlike the GDPR, the DP Law does not provide a specific legal basis for processing and/or anonymising health data for scientific purposes. Under the DP Law, (i) the processing of personal data for purposes such as research, planning, and statistics through anonymisation, and (ii) the processing of personal data for scientific purposes, provided that it does not violate national defence, national security, public security, public order, economic security, the right to privacy, or personality rights, and does not constitute a criminal offence, are completely exempt from the application of the DP Law. Moreover, according to the By-law on Personal Health Data, health data may be used for scientific purposes when the exemptions in the DP Law are triggered.

However, since (i) the DP Law does not define scientific research, and (ii) the DPA has not adopted a clear

stance on the application of this exemption to health data processing for scientific purposes, relying on this exemption may not be possible, especially considering the commercial nature of such activities, which creates legal uncertainty.

In terms of the open health data space, the By-law on Personal Health Data stipulates that the data contained in systems used by organisations affiliated with the Ministry of Health, with a consideration on regulations related to data privacy and security, shall be made accessible to everyone through a dedicated website with the aim to ensure transparency and accountability in the healthcare system, guide policies and strategies for healthcare service delivery, support scientific research in the health sector, and facilitate the development of health-related products and services.

Lastly, according to the By-law on the Protection and Processing of Data Within the Social Security Institution (SSI), data obtained by the SSI may be anonymised and transferred upon the Institution's approval, for purposes such as the development of health and social security policies, the protection of public health, the preparation of statistics, and scientific or academic research.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Türkiye does not currently have an AI law but is focused on regulating AI in the future, setting goals for a comprehensive legal framework and AI governance in line with international trends, including the EU's AI Act, as outlined in its strategy documents. In addition, the DP Law does not establish a specific regime for processing activities carried out through AI systems.

However, the DPA has issued specific guidance titled “the Guideline on Generative Artificial Intelligence and Personal Data Protection (AI Guideline)”. The AI Guideline provides clarifications on how to ensure compliance with the DP Law in processes involving generative AI. The AI Guideline provides recommendations aimed at facilitating transparency in the development, deployment, and use of generative AI, and it recommends a human oversight mechanism, but it does not establish a risk-based regime. Consequently,

the AI Guideline serves as a resource for those developing, deploying, and using generative AI. However, a few statements in the AI Guideline appear to have potential to give rise to uncertainty in practice.

The DPA has also published a guidance titled “Use of Generative AI Tools in Workplaces”, which highlights key risks related to the use of third-party generative AI tools, such as data protection, information security, trade secrets, and inaccurate outputs, and provides governance recommendations for companies, without introducing specific legal obligations.

Lastly, in March 2026, the DPA accomplished a guideline in AI governance by issuing its Guideline on Agentic Artificial Intelligence “Agentic AI Guideline”, indicating DPA's growing emphasis on setting clarity for autonomous systems. The Board's dedication to providing more clarity through technical definitions and classifications, such as the distinction between integrated Agentic AI systems and task-specific AI Agents, is demonstrated in the Agentic AI Guideline. The Agentic AI Guideline is firmly based on the Law's core data protection principles, even if it provides a more detailed examination of these technologies through sectoral examples in healthcare and finance. The DPA gives organisations a road map for navigating data controller responsibilities in the era of digital agents by reiterating that even the most autonomous systems must adhere to fundamental obligations, such as transparency, purpose limitation, and human oversight, rather than departing from accepted norms.

1.6 Data Breach Requirement

There is no explicit definition of “data breach” under the DP Law. However, the obligation to notify the DPA arises “in the event that personal data is obtained by others through unlawful means”, pursuant to the DP Law. Considering this explicit provision, it can be interpreted that data breach notification under the DP Law is limited solely to the breach of the data's confidentiality; therefore, it could be argued that, unlike the GDPR, the loss of data integrity or availability is not regulated as a breach that triggers a notification obligation within the framework of the DP Law.

Despite this, it is observed that in the DPA's Breach Notification Form, “data integrity” and “data access/

availability” elements are also evaluated under the heading of Breach Impact, indicating that the DPA interprets this concept broadly.

Controllers are required to notify the DPA without delay and no later than 72 hours after becoming aware of the breach. Additionally, controllers must inform affected data subjects as soon as possible, with the necessary details regarding the breach and the potential risks to their personal data. The DP Law does not establish risk thresholds for assessing the requirement to notify the breach to the DPA and the data subjects, meaning that every breach must be reported, regardless of its perceived risk level.

In terms of supervision, written audits are typically preferred by the DPA over on-site inspections, although the DPA is entitled to conduct the latter. After reporting the breach to the DPA, controllers should keep an internal breach log and be prepared for any ex officio inquiries. Immediate internal documentation, prompt official notifications, and the compilation of technical evidence for written regulatory inquiries are important action items.

Additionally, the Cybersecurity Law obliges those who provide services, collect data, process data, or conduct similar activities using information systems to notify the Cybersecurity Presidency, without delay, of any vulnerabilities or cyber incidents they detect in the field in which they provide services. Therefore, when controllers suffer a personal data breach, the breach will most likely also be notified to the Cybersecurity Presidency.

1.7 Regulators

The primary supervisory and regulatory authority is the DPA. It is an independent administrative institution.

The DPA regulates data protection activities and safeguards the rights of data subjects. Some of its duties and powers are as follows:

- conducting investigations and taking temporary measures;
- concluding the complaints;
- imposing administrative sanctions;
- issuing adequacy decisions; and

- approving transfer mechanisms that require DPA approval.

The Ministry of Trade is authorised to oversee marketing communications (see **4.2 Personalised Advertising and Other Online Marketing Practices**).

Additionally, sector-specific administrative institutions as the Banking Regulation and Supervision Agency, the Capital Markets Board, the Turkish Republic Central Bank, and the Cybersecurity Presidency have the authority to regulate issues within their respective sectors.

1.8 Enforcement Proceedings and Fines

The DPA may initiate investigations upon receiving a complaint from a data subject or ex officio if it becomes aware of the alleged violation.

The Course of an Investigation

The DPA may request information and/or documents from controllers. Controllers are required to provide requested information and/or documents within 15 days, unless they constitute a state secret. The DPA may request additional information and/or documents and conduct an on-site inspection during an investigation.

Administrative Fines

The DP Law outlines five types of violations, each subject to administrative fines that are adjusted annually. As of 2026, they are:

- failure to inform data subjects of processing activities (between TRY85,437 and TRY1,709,200);
- failure to take the necessary technical and organisational measures (interpreted broadly, including unlawful data transfer abroad and breach of fundamental principles) (between TRY256,357 and TRY17,092,242);
- failure to comply with the decisions issued by the DPA (between TRY427,263 and TRY17,092,242);
- failure to comply with the obligation to register with VERBIS and failure to submit information to VERBIS (between TRY341,809 and TRY17,092,242); and

- failure to notify the DPA within five business days following the signature of the standard contracts (SCCs) (between TRY90,308 and TRY1,806,177).

Unlike other failures stipulated in the DP Law where only the controller is responsible, both controllers and processors can be held liable for failure to notify the DPA regarding SCCs.

The DPA must consider the severity of the breach, the fault of the breaching party, and its economic condition.

Administrative Orders

The DPA may also order controllers to bring their processing activities into compliance with the DP Law. When the DPA issues such an order, this decision must be implemented without any delay and, at the latest, within 30 days upon receipt of the notification by the controller.

The DPA is also entitled to cease certain personal data processing activities or transfers abroad if it finds that such processing activities result in damages that are difficult or impossible to compensate for, and if the act is clearly unlawful.

Appeal Mechanisms

Controllers have the right to appeal against the DPA's decisions. They may object to such decisions before the administrative courts within 60 days of receiving the decision.

The decisions of the administrative courts can be appealed to the Regional Administrative Courts, and the decisions of the Regional Administrative Courts can be further appealed to the Council of State, provided that the administrative fine exceeds the applicable thresholds.

However, if the DPA's decision includes only an administrative measure rather than an administrative fine, decisions of both the administrative courts and Regional Administrative Courts can be appealed, regardless of the relevant minimum thresholds.

Civil Orders

A data subject who suffers damage due to the unlawful processing of their personal data under the DP Law has the right to seek compensation by applying to the competent civil court.

Criminal Orders

The TCrC governs criminal liability for data-related offences. Under the TCrC, unlawful recording of personal data is punishable by imprisonment from one to three years. Article 136 stipulates that any individual who unlawfully provides, disseminates, or obtains personal data shall face a prison sentence of two to four years. Article 138 addresses the failure to destroy personal data; if a person responsible for data management fails to delete or anonymise personal data despite the expiry of legally mandated retention periods, they are subject to imprisonment for one to two years.

Enforcement Under the Cybersecurity Law

The Cybersecurity Presidency is still being established and has not yet initiated any enforcement actions. However, according to the Cybersecurity Law, the Cybersecurity Presidency is entitled to conduct on-site inspections, request information and technical materials, and examine systems; in certain cases, searches, copying, and seizure require a judge's decision or, in urgent cases, a prosecutor's written order, subject to prompt judicial approval. Administrative fine decisions may be challenged before the administrative courts. The law does not provide a settlement mechanism.

Sanctions include both administrative fines and criminal penalties. Administrative fines apply, for failing to report vulnerabilities or cyber incidents, failing to meet procurement/certification obligations, and obstructing audits, among others; in some cases, fines for companies may reach up to 5% of annual gross sales. Criminal sanctions include imprisonment and judicial fines for withholding requested information, operating without required approvals, breaching confidentiality, unlawfully disclosing leaked data, spreading false leak claims, carrying out cyber-attacks, or abusing statutory powers. Penalties are generally shaped by the nature of the breach, repetition, any benefit gained, or damage caused, turnover where relevant, and aggra-

vating factors such as commission by public officials, multiple offenders, or organised groups.

1.9 Enforcement Trends

The DPA has focused on specific topics and issued important decisions and announcements regarding its actions.

Loyalty Programmes and In-Store Consent Practices

The DPA emphasises the importance of authentication mechanisms in loyalty programmes, requiring controllers to verify whether the person using the loyalty account during a purchase is the account holder. Additionally, the DPA emphasises that SMS verification codes used during purchases or service processes must not be misleadingly presented as mandatory if they also serve purposes such as obtaining consent for data processing or commercial communications.

Online Protection of Minors

The DPA has initiated an ex officio investigation into several social media platforms to examine how children's personal data are processed and what safeguards are implemented. The investigation aims to assess whether adequate measures are in place to protect children from potential risks in the digital environment, considering the best interests of the child and the need to ensure protection of their personal data when using social media services.

Focus on AI

Although it has not yet resulted in an enforcement action, the DPA has issued several guidelines regarding the use of AI.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Tracking privacy litigation trends in Türkiye is challenging, due to the limited accessibility of case law. Only Constitutional Court decisions are required to be published in the Official Gazette, while decisions from other courts remain largely unpublished. This lack of transparency makes it challenging to predict how data protection laws will be interpreted and applied by the

courts, hindering the ability to identify clear trends in privacy litigation at this stage.

In recent years, the court has rendered a limited number of decisions directly concerning personal data, primarily focusing on the exercise of the rights to deletion and rectification, as well as the overall effective protection of data privacy.

A notable decision by the court addressed the protection of personal data within the context of inaccurate judicial records. In this case, the court held that the refusal to delete a citizen's status as a "complainee" from the National Judiciary Network Information System, despite the formal absence of an actual complaint, constituted a violation of the right to request the rectification of personal data. The court further emphasised that the failure of judicial authorities to conduct a substantive review of the rectification request effectively deprived the individual of an effective legal remedy.

Another significant ruling by the Constitutional Court clarified the State's positive obligations regarding the ineffective investigation of unlawful personal data acquisition and use between private individuals. The court ruled that a superior's use of a subordinate's personal records – such as union membership forms and internal petitions – as evidence in a private lawsuit violated the right to data protection. This was confirmed by the fact that the institution holding the data had never transferred it to the judiciary, and therefore the data was obtained without administrative action or explicit consent.

The DP Law refrains from establishing specific provisions for the compensation of damages arising from the unlawful processing of personal data and makes no distinction between material and moral harm. Instead, it stipulates that the right to compensation for those whose personality rights are violated is reserved under general provisions, while the TCiC explicitly allows for both material and moral claims in such instances. To seek damages based on a violation of the DP Law, the absence of legal justification, a breach of the data controller's duty of care, and a clear causal link between the unlawful act and the resulting harm must be established. Regarding compensation

for moral damages, a causal link between the unlawful attack and the moral damage is required.

2.2 Recent Case Law

Due to the lack of transparency (see 2.1 **Privacy Litigation Overview**), a concrete determination regarding the existing case law cannot be made. As such, it is not always possible to determine which privacy lawsuits are currently ongoing or to identify landmark cases.

In practice, it is known that legal remedies have been pursued against the decisions and administrative fines imposed by the DPA. However, tracking these cases is not always feasible and, therefore, it would be appropriate to state that no standout cases have been identified.

Both ordinary and extraordinary legal remedies have been pursued against the decisions and administrative fines imposed by the DPA within the framework of the DP Law, as well as under legislation relating to the right to data protection. For instance, ongoing legal proceedings exist relating to the crime of unlawful recording of personal data under the TCrC, as well as civil proceedings under the TCiC concerning the prevention of and/or compensation for unlawful processing of personal data as a violation of personal rights.

An example, recently issued by the Turkish Supreme Court, is a decision addressing moral compensation claims arising from the unauthorised disclosure of banking records and personal data by a financial institution. The court argued that the bank, acting as a “trust institution” and as the data controller, violated the principles of “purpose limitation” and “data minimisation” by submitting extensive account movements that exceeded the specific timeframe requested by the judiciary. It further stated that such an unlawful disclosure constituted a direct violation of the data subject’s personality rights and emphasised that the subsequent publication of this data by third parties did not break the causal link between the bank’s negligence and the resulting moral damage.

2.3 Collective Redress Mechanisms

There is no concept of collective redress for privacy litigation under the Turkish legal system, nor have there been any developments in this area.

That said, associations and other legal entities may file lawsuits on behalf of their members or the group of people they represent, to protect their interests, address unlawful situations, or prevent future violations. For instance, under the Turkish Consumer Protection Law consumer organisations, relevant public institutions and the Ministry of Trade may take legal action before the consumer courts to prevent or halt unlawful situations affecting consumers, excluding unfair commercial practices and advertisements. However, these provisions do not explicitly address collective actions related to privacy.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Unlike the EU Data Act, there is no specific regulation addressing non-personal data in Türkiye. General rules apply.

As for future endeavours, the 12th Development Plan (2024–2028), states that a national data governance framework will be established and the necessary technical, institutional, and legislative infrastructure will be developed.

Additionally, the Medium-Term Programme (2026–2028), sets the development of a governance framework that safeguards data privacy and security as a goal, and states that the National Data Strategy and Action Plan will be implemented in the third quarter of 2026.

3.2 Interaction of Data Regulation and Data Protection

Since there are no specific standalone data regulations, general rules apply.

3.3 Rights and Obligations Under Applicable Data Regulation

Due to the absence of a standalone regulation specifically addressing the use of non-personal data, general obligations outlined in the DP Law apply in so far as these services involve processing of personal data (see 1.2 Rights and Obligations).

3.4 Regulators and Enforcement

As Türkiye currently lacks comprehensive data regulations beyond those pertaining to personal data protection, there is no specific regulatory body solely tasked with enforcement in this area. However, when relevant actors process personal data, the DPA will be responsible for overseeing the process. That being said, sector-specific regulations may grant authority to certain regulatory bodies over specific data-related matters.

4. Sectoral Topics

4.1 Use of Cookies

Under Turkish law, there is no legislation explicitly governing the use of cookies, except for the Electronic Communications Law (ECL), which applies only to electronic communications service providers. The ECL permits cookies for communication or if users are informed and give explicit consent.

The DPA considers data collected through cookies as personal data, thus subject to the DP Law. The DPA issued the Guidelines on Cookie Applications (Cookie Guidelines) providing best-practice recommendations for data controllers, including cookie banners, consent management platforms, and a sample cookie policy.

Cookie Guidelines is limited to the use of cookies and does not cover other tracking technologies such as Software Development Kits (SDKs) and device identifiers. However, as the DPA has not issued specific guidance on the latter and given their similar processing nature, the Cookie Guidelines may also serve as an important reference in terms of the DPA's approach to tracking technologies other than cookies.

The Cookie Guidelines also refer to the ECL and provide two criteria for processing activities where

controllers rely on legitimate interest. Controllers are advised to perform a balancing test, weighing the individual's rights and freedoms against the controller's legitimate interests, taking into account whether:

- cookies are essential for communication via electronic communication networks; or
- cookies are strictly necessary for information society services explicitly requested by the user.

Moreover, the Cookie Guidelines include several recommendations for situations where controllers obtain data subjects' explicit consent for the use of cookies, for which an opt-in mechanism is required. For instance, using consent management platforms allowing data subjects to manage their preferences is cited as a good practice. However, since frequent requests may cause "consent fatigue", consent reminders are advised to align with the cookie's lifespan.

Furthermore, consent obtained through cookie walls – where access to a website is conditioned on accepting cookies – is generally considered invalid if it prevents users from making a genuine choice. However, a cookie wall may be deemed acceptable on a case-by-case basis, provided that fair alternatives are offered to the user for accessing the service without compromising their free will.

In cases where the use of cookies involves transferring data abroad, controllers should also consider the requirements outlined in the DP Law (see 5.1 Restrictions on International Data Transfers).

Special Considerations for Analytics Cookies

The Cookie Guidelines classify cookies by duration, purpose and party. While these categories largely mirror EU practice, there is a key difference for analytics cookies; explicit consent may not be required for first-party analytics cookies, provided that:

- their use is limited to measuring site or application's target audience;
- personal data collected through cookies – which are not strictly required for the purpose of processing – is anonymised;
- the personal data collected through cookies is only used for anonymous statistics;

- the duration of cookies is reasonable, and personal data collected is not transmitted to third parties.

In this scenario, personal data collected through cookies should not be used to track users across multiple sites or devices.

Non-essential cookies are subject to strict opt-in requirements. Organisations must seek explicit consent before using cookies and SDKs for advertising, marketing, or performance-tracking purposes. In contrast, necessary cookies follow an opt-out paradigm, which means they can be used without agreement as long as clear information is provided and an opt-out option is accessible for the users.

4.2 Personalised Advertising and Other Online Marketing Practices

Online Marketing

Online marketing is mainly governed by the Law on Regulation of Electronic Commerce, the By-law on Commercial Communication and Commercial Electronic Messages (together “E-Commerce Legislation”), and the DP Law.

According to the E-Commerce Legislation, prior approval from recipients must be obtained before making calls or sending SMS or emails for marketing purposes (marketing communications). This approval is a specific authorisation for sending marketing communications and is distinct from the explicit consent required under the DP Law for processing personal data for marketing purposes. Although the Ministry of Commerce, which oversees compliance with the E-Commerce Legislation, does not consider push notifications as marketing communications, the DPA requires data subjects’ explicit consent to send push notifications. The Ministry of Trade has decided that enabling push notifications on a phone does not by itself constitute consent for marketing messages and that users must be given the option to receive only informational notifications.

The E-Commerce Legislation provides an exemption for marketing communications sent to tradespeople or craftspeople in the business-to-business (B2B) context, where their approval is not required, but they must be given the option to opt out.

Marketing communications must include the sender’s precise identification information, as well as an option to opt out.

All senders of marketing communications are required to register with the Message Management System (MMS) and upload information regarding the approvals and withdrawals for this purpose. MMS is an online platform where recipients can manage their approvals for receiving marketing communications and opt out if desired. Any approval or withdrawal received by the sender must be uploaded to the MMS within three business days of receipt.

Personalised Advertising

Turkish law does not have specific provisions for behavioural and targeted advertising. Therefore, these activities are subject to general provisions of the DP Law. In line with the DPA’s general approach to this matter, in principle, prior explicit consent from data subjects is required for behavioural or targeted advertising.

That being said, as far as it is known, the DPA has ruled in an unpublished decision that, in specific cases, controllers may rely on legitimate interest for behavioural or targeted advertising. However, as the details of this decision have not been published, the DPA’s rationale behind this decision remains unclear.

Unlike the Digital Services Act, Turkish law does not include specific restrictions on the profiling of minors for online advertising. Nevertheless, as mentioned in **1.9 Enforcement Trends**, the online protection of minors is a trending topic for the DPA, and additional obligations in this area may be expected in the future.

4.3 Employment Privacy Law

Employment privacy is not governed by a specific, standalone regulation in Turkish law. However, some provisions related to employment privacy are included in diverse laws, such as:

- the TCO provides that an employer may use an employee’s personal data only to the extent necessary for the employee’s employability or the performance of the employment contract;

- Turkish Labour Law obliges employers to handle information obtained about their employees under the rules of good faith and law and prohibit disclosing any information that the employee has a justified interest in keeping confidential;
- Occupational Health and Safety Law mandates that health data must be kept confidential to protect the private life and reputation of the employee.

Essentially, the general principles of the DP Law apply in the workplace and controllers must comply with its obligations. However, due to the unique relationship between employers and employees, controllers face certain challenges in practice.

Monitoring Workplace Communications

In some of its decisions, the DPA addressed the monitoring of employee communications in the workplace. Accordingly, an employer is entitled to monitor work computers, work mobile phones, and other electronic devices provided to employees, provided that the following conditions are met:

- informing employees in advance;
- pursuing a legitimate purpose; and
- observing the principle of proportionality.

These principles also apply to the implementation of cybersecurity tools.

The Constitutional Court addressed this issue in several decisions. In one case, an employer examined an employee's corporate email and used the correspondence to terminate the employment contract. The court highlighted that the contract specified the corporate email was for work purposes and could be monitored without prior notice. It emphasised that using the emails for legal purposes in a judicial process was reasonable and proportionate. In another case, holiday pictures and emails sent from the corporate email were used as evidence in the judgment.

Essentially, the Constitutional Court appears to consider the following criteria for employers when monitoring employees' communication tools:

- the terms governing the use of work equipment;
- employee awareness of these terms;

- the proportionality of the interference with employees' rights; and
- whether contract termination is reasonable in light of the employee's actions.

Obtaining Explicit Consent

Employees' explicit consent may not always be considered valid, as employees may not have complete freedom in their relationship with their employer due to the imbalance of power between the parties. Therefore, controllers should carefully assess whether the requirements for explicit consent are met, particularly for processing activities within an employment relationship.

This does not mean that explicit consent obtained from employees will always be deemed invalid. In a decision involving a controller based abroad that obtained employees' personal data through its liaison office, the DPA clarified that employees' explicit consent for the transfer of personal data abroad may be considered valid, as the employee understands that their data will ultimately be processed by the controller abroad.

Processing Special Categories of Personal Data

Before the DP Law Amendments, the legal bases for processing special categories of personal data were limited, creating challenges for controllers, particularly employers processing health data in an employment context. Especially, the introduction of a legal basis allowing the processing of employees' health data where "for the fulfilment of legal obligations in the fields of employment" has significantly facilitated the lawful processing of such data by controllers.

Background Checks

Records related to criminal convictions are considered special categories of personal data under the DP Law. Thus, processing criminal convictions for background checks is considered the processing of special categories of personal data. There is debate over whether employers can process this information based on explicit consent or if it can be processed under the legal basis of "necessity for fulfilling legal obligations in employment". The DPA's Guidelines on the Processing of Special Categories of Personal Data states that decisions such as criminal convictions, imprisonment,

conditional release, judicial fines, or revocation of a driver's licence are considered processing of special categories of personal data. Therefore, some interpretations in the sector suggest that processing criminal record documents showing a clear background (ie, no convictions) does not count as processing special categories of personal data.

Processing for Job Applications

The DP Law does not provide a specific regime regarding the processing of job applications, and general provisions apply. In this regard, personal data related to a job application can be processed without explicit consent based on the legal basis of "processing is necessary for establishment or performance of the contract". However, the data must be stored only for the purpose of which it was processed. Data of the candidate who is not selected should be deleted after reasonable period.

4.4 Data Protection in M&A

As the DP Law does not explicitly regulate M&A transactions, such processes are governed by the general principles of the DP Law. Key requirements can be categorised as follows:

Due Diligence Phase

- **Legal Basis:** Controllers must ensure they rely on the appropriate legal bases outlined in the DP Law when transferring personal data.
- **Data Minimisation:** Sellers must redact or anonymise personal data whenever possible. Data-sharing should be strictly limited to what is necessary for the transaction's valuation and legal assessment.
- **Data Rooms:** Access must be restricted on a "need-to-know" basis. Data rooms should use pseudonymisation, redaction, or anonymisation where feasible.
- **Data Protection Compliance Audit:** A holistic audit must be conducted to evaluate the target company's compliance with data protection laws.

Notification

- **Data Subjects:** Data subjects must be informed about the data processing and transfer activities. In cases where the transfer relies on explicit consent,

the data controller must ensure that explicit consent should be obtained.

- **VERBIS:** The DPA must be informed by any changes of the controller's representative or contact information.
- **Data Transfers Abroad:** If the buyer is a foreign entity and the data is being transferred to servers outside of Türkiye, the parties must comply with the DP Law, which may require SCCs which are subject to notification to the DPA.

Post-Closing Phase

- **Data Migration and Security:** During the technical migration of databases, the buyer must implement robust technical and organisational measures, including encryption and access logs, to safeguard data confidentiality and integrity.

5. International Considerations

5.1 Restrictions on International Data Transfers

With the DP Law Amendments, the previous system has been significantly amended. Current provisions of the DP Law foresee a gradual and alternative regime for international transfers, comprising three levels based on;

- adequacy decisions;
- appropriate safeguards; and
- occasional causes.

While the DP Law does not include a definition of "data transfer abroad", the By-law on Data Transfers Abroad fills this gap by defining it as "the transmission of personal data by a data controller or data processor within the scope of the DP Law to a data controller or data processor abroad or making it accessible by any other means".

With its Guidelines on Transfers Abroad, the DPA further clarified that direct collection of personal data does not constitute data transfer under the new regime, in contrast to its previous position.

Adequacy Decisions

Adequacy decisions provide a valid legal basis for transferring data abroad. The DPA has the authority to issue adequacy decisions not only for countries but also for international organisations and specific sectors within third countries (a “Whitelist”).

Adequacy decisions must be reviewed by the DPA at least once every four years. If the DPA determines that adequate protection is no longer ensured, these decisions may be amended, suspended, or revoked with prospective effect following the review, or in any other cases it deems necessary.

Since the DPA has not yet established a Whitelist, alternative mechanisms for transferring data abroad must be considered in practice.

Appropriate Safeguards

In the absence of an adequacy decision, data transfers abroad can still occur through the implementation of appropriate safeguards. However, these safeguards can only be utilised if the conditions for processing personal data are met, and if it is feasible for data subjects to exercise their rights and access effective legal remedies in the third country where the data will be transferred.

There are four methods to deploy appropriate safeguards:

- an agreement between “public institutions and organisations or international organisations abroad” and “public institutions and organisations or public professional organisations in Türkiye”, subject to the DPA’s approval;
- binding corporate rules (BCR), subject to the DPA’s approval;
- a written undertaking containing provisions that will provide adequate protection, subject to the DPA’s approval; and
- SCCs announced by the DPA, with a requirement for notification to the DPA within five business days from the execution date. The By-law on Data Transfers Abroad states that notifications of SCCs can be made physically, via registered electronic mail, or through other methods determined by the

DPA. In this context, the DPA introduced an online “SCC Notification Module” in 2024.

Due to the challenges in obtaining approval from the DPA, SCCs have been the most viable option in market practice.

The DPA published SCCs modules that cover data transfers from (i) controller to controller, (ii) controller to processor, (iii) processor to processor, and (iv) processor to controller.

While the English-language versions are also available on the DPA’s website, the By-law on Data Transfers Abroad clearly emphasises that if SCCs are executed in a foreign language, the Turkish version will prevail. This is further confirmed in the Guidelines on Transfers Abroad, stating that double-column SCCs will be considered valid by the DPA, provided that the Turkish version is properly executed.

The SCCs published by the DPA must be executed without any modification, except where explicitly allowed within the relevant sections of the SCCs. While various practices emerged due to uncertainties arising from the lack of guidance, the Guidelines on Transfers Abroad provided clarifications on how to complete each section of the annexes to be filled out by the parties. For instance, while many practitioners only included the categories of personal data transferred, the guidelines clarified that both the categories and the specific data transferred should be stated.

The notifications should include:

- the final version of the SCCs, with relevant sections filled out and signed by authorised individuals of the parties;
- documents proving authority of those signing the SCCs;
- notarised translations of foreign-language documents.

The Guidelines on Transfers Abroad also confirmed that official documents from foreign authorities can be included in the notification, with authentication of signatures, titles, or seals required. This verification is usually done by consular or diplomatic officials. How-

ever, under the Convention Abolishing the Requirement of Legalisation for Foreign Official Documents, documents from signatory countries are exempt from this process, and an apostille is sufficient.

Occasional Transfers

If data transfers abroad cannot occur with an adequacy decision, and if one of the appropriate safeguards cannot be ensured, the data transfer abroad is possible if the transfer is occasional and one of the legal bases laid down for occasional transfer is met.

The By-law on Data Transfers Abroad defines occasional transfers as “transfers that are not regular, occur only once or a few times, are not continuous, and are not in the ordinary course of business”. Examples, largely based on EDPB guidelines, are provided in the Guidelines on Transfers Abroad.

When relying on explicit consent for an occasional transfer, the data subject must be informed of the specific risks, including that the destination country may not provide adequate protection or implement sufficient security measures. This may involve the absence of a supervisory authority or guarantees for data processing principles and individual rights.

Onward Transfers

It should be noted that the requirements regarding personal data transfer abroad also extend to onward transfers conducted by either controllers or processors.

Other Regulations

The DP Law states that provisions on data transfers abroad in other laws are reserved. The Guidelines for Good Practices on Personal Data Protection in the Banking Sector emphasise that specific provisions outlined in the Banking Law should be considered when transferring information that constitutes client secrets abroad. Likewise, the By-law on Measures for Preventing Money Laundering and Financing of Terrorism provides details on the required information that must be included in an international e-transfer, adding further compliance obligations for financial institutions.

Sectoral regulations imposing specific restrictions regarding data transfers abroad should also be considered.

5.2 Government Notifications and Approvals

As detailed under 5.1 Restrictions on International Data Transfers, data transfers abroad can occur through the implementation of appropriate safeguards and, except for SCCs, these safeguards require the DPA’s prior approval.

Furthermore, without prejudice to the provisions of international agreements, in cases where the interest of Türkiye or the data subject will be seriously harmed, personal data may only be transferred abroad with the permission of the DPA. The DPA must obtain the opinions of relevant public institutions and organisations before it grants its permission.

Sector-specific regulations may also require further notifications or approvals. For instance, under the Regulation on Geographic Data Permissions, transferring geographic data is subject to the authorisation from the Ministry of Environment, Urbanisation, and Climate Change.

In the health sector, the transfer of personal health data is subject to the evaluation of the Ministry of Health under the By-law on Personal Health Data. Similarly, in the civil aviation sector, airline operators or institutions may share passenger information with third countries upon request under the Turkish Civil Aviation Law, provided that they obtain approval from the Ministry of Interior.

5.3 Data Localisation Requirements

While there is no standalone legislation governing data localisation, certain sector-specific regulations do apply. Key sectors include:

Banking and Finance Entities

The following entities must keep their primary and secondary information systems in Türkiye:

- banks;
- payment institutions and electronic money institutions;
- insurance and private pension companies;

- capital markets institutions; and
- financial leasing, factoring, and finance companies.

Electronic Communications Providers

In principle, electronic communications providers cannot transfer traffic and location data abroad, for national security reasons. In certain cases, such data may be transferred abroad by obtaining the explicit consent of data subjects.

Specific requirements for obtaining consent from users are further regulated in secondary legislation. For instance, in cases where traffic and location data will be transferred, users must be informed about the scope of the data to be transferred, the name and address of the recipient party, the purpose and duration of the transfer, and, if the third party is located abroad, the name of the country to which the data will be transferred, at the time of obtaining their consent.

In 2019, the Information and Communication Technology Authority (ICTA) mandated that all infrastructure, systems, and storage units related to eSIM technologies, including eSIM subscription management, must be set up in Türkiye either by operators authorised in Türkiye or by third parties designated by the operators, with the operator bearing full responsibility. Additionally, any data generated through eSIM technologies must be stored in Türkiye.

Social Network Providers (SNPs)

SNPs with daily access exceeding one million must implement the necessary measures to ensure that the data of their Turkish users is retained within Türkiye. The ICTA further emphasised that priority should be given to storing essential user data, along with any other data specified.

Commercial Electronic Message Management System Integrators

The Communique on Commercial Electronic Message Management System Integrators mandates that authorisation from the Ministry of Trade is required to act as an integrator for service providers in registering approvals and rejections of marketing communications in the MMS, or to carry out these transactions through the MMS. The communique stipulates that the information processing system used in integra-

tor services, including software, hardware, and server infrastructure, must be located within a local database.

Critical Infrastructure Service Providers

The Decree on Information and Communication Security Measures issued by the Presidency of Türkiye (Presidency Decree), sets specific measures to mitigate security risks, particularly for critical data that could jeopardise national security or public order if compromised. It provides an obligation to store critical data (eg, population, health, and communication records, genetic and biometric data) securely.

The Presidency Decree applies not only to businesses providing critical infrastructure services (eg, energy, electronic communications, banking, transportation) but also to public institutions and organisations.

It stipulates that data from public institutions must not be stored in cloud services unless hosted in the institutions' own private systems or with local service providers under their control.

5.4 Blocking Statutes

Türkiye does not have specific "blocking" statutes, but there are general statutory provisions to prevent the disclosure of matters relating to national interests.

5.5 Recent Developments

Following the most recent amendments to the DP Law, the DPA has made efforts to clarify the recently amended international personal data transfer regime with the Guidelines on Transfers Abroad and the announcement on the "Key Considerations for Standard Contracts to be Used in the Transfer of Personal Data Abroad".

The DPA has recently made an announcement regarding the use of foreign messaging applications in public institutions. The DPA emphasised that official documents containing confidential or critical data should not be shared through such applications, considering that these applications do not have data centres within the country.

The DPA has also announced that an agreement (not qualifying as an international treaty) between the Min-

istry of the Interior's Directorate General of Migration Management and the United Nations High Commissioner for Refugees, which serves as the basis for the transfer of personal data abroad, was reviewed and authorised.

Furthermore, efforts to align with the GDPR are ongoing. According to the Medium-Term Programme (2026–2028), the alignment of the DP Law with the GDPR and other EU legislation is expected to be completed by the third quarter of 2026. Additionally, the 12th Development Plan (2024–2028) identifies alignment efforts as a key goal for the coming years.



Law and Practice

Contributed by:

Saifullah Khan and Saeed Hasan Khan
Bizilance Legal Consultants

Contents

1. Legal and Regulatory Framework p.530

- 1.1 Overview of Data and Privacy-Related Laws p.530
- 1.2 Rights and Obligations p.530
- 1.3 Special Categories of Personal Data p.531
- 1.4 Processing of Personal Data for Research and Development Purposes p.532
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.532
- 1.6 Data Breach Requirement p.532
- 1.7 Regulators p.533
- 1.8 Enforcement Proceedings and Fines p.533
- 1.9 Enforcement Trends p.534

2. Privacy Litigation p.534

- 2.1 Privacy Litigation Overview p.534
- 2.2 Recent Case Law p.534
- 2.3 Collective Redress Mechanisms p.534

3. Requirements for the Protection and Processing of Non-Personal Data p.534

- 3.1 Objectives and Scope of Data Regulation p.534
- 3.2 Interaction of Data Regulation and Data Protection p.535
- 3.3 Rights and Obligations Under Applicable Data Regulation p.535
- 3.4 Regulators and Enforcement p.535

4. Sectoral Topics p.535

- 4.1 Use of Cookies p.535
- 4.2 Personalised Advertising and Other Online Marketing Practices p.536
- 4.3 Employment Privacy Law p.536
- 4.4 Data Protection in M&A p.536

5. International Considerations p.536

- 5.1 Restrictions on International Data Transfers p.536
- 5.2 Government Notifications and Approvals p.537
- 5.3 Data Localisation Requirements p.537
- 5.4 Blocking Statutes p.537
- 5.5 Recent Developments p.537

Bizilance Legal Consultants practises in the areas of trade remedy law, privacy and data protection, taxation, and antitrust and competition, among others. The firm is backed by the rich experience of its directors, spanning over two decades. The directors have served clients in multiple jurisdictions, including the UAE, the USA, the UK, KSA, Switzerland, Sin-

gapore, China, Malaysia, Indonesia, Korea, Thailand and Pakistan. In the personal data and privacy space, Bizilance Legal Consultants at Abu Dhabi Global Market is strategically well placed to serve multi-jurisdictional clients in an era when laws related to personal data protection have either just been implemented or are in the process of being implemented.

Authors



Saifullah Khan is an international trade, IT and policy lawyer with more than 23 years of diversified and multi-jurisdictional professional experience in serving a large client base in the domestic and international

markets. His areas of interest include WTO trade remedy laws, customs law, competition law and data privacy. Regarding the emerging discipline of data privacy, he advises clients from different jurisdictions about data privacy compliance and cross-border transfer of data. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on “Data: Law, Policy and Regulation”.



Saeed Hasan Khan has more than 23 years' experience in advising and representing clients on issues such as taxation, corporate, regulatory compliance and contractual obligations. He has developed a keen

professional interest in emerging laws on personal data protection, and an understanding of the underlying concepts and principles governing global data protection laws, including the EU's GDPR. He has carried out considerable research on personal data protection laws in various jurisdictions. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK), holds CIPP/E certification and is a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on “Data: Law, Policy and Regulation”.

Bizilance Legal Consultants

D 3 - 4
Office 302
Al Sarab Tower
Level 15th
ADGM Abu Dhabi
United Arab Emirates

Tel: +971 52 914 1118
Email: saeed.hasan@bizilancelegal.ae
Web: www.bizilancelegal.ae

Bizilance
Legal Consultants

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Constitution of the United Arab Emirates (UAE) provides that safety and security for all citizens shall be the pillars of society. The Constitution further provides that freedom of correspondence by post, telegraph or other means of communication, and the secrecy thereof, is guaranteed in accordance with the law, and that dwellings are inviolable. These constitutional provisions serve as the foundational guidelines for respecting privacy.

The statutory regime concerning data protection is chiefly found in the following laws/regulations.

Federal Decree Law No 45 of 2021 on personal data protection (the “UAE Law”)

The UAE Law is a federal-level law applicable across the UAE, except for the following:

- governmental data;
- government authorities that control and process personal data;
- security and judicial authorities;
- health-related personal data;
- banking and credit personal data; and
- companies and organisations incorporated

Dubai International Financial Centre (DIFC) Law No 5 of 2020 (the “DIFC Law”)

The DIFC is a free zone, and the DIFC Law applies in the jurisdiction of the DIFC to the processing of personal data, regardless of the place of incorporation of the controller or processor. Similarly, it is also applicable to controllers and processors incorporated in the DIFC, irrespective of their processing of personal data.

The Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (the “ADGM Regulations”)

The ADGM is a free zone, and the ADGM Regulations apply in the context of the establishment of a controller or a processor in the ADGM.

Apart from the above, sector-specific regulations govern data protection in their respective sectors, as follows:

- Federal Decree-Law No 6/2025 Concerning the Central Bank and the Regulation of Financial Institutions, Activities, and Insurance Business (governing data protection of customers of banks);
- Federal Law No 3 of 2003 (concerning telecommunications) governing data protection of telecoms consumers; and
- Federal Law No 2 of 2019 (concerning use of information and communication technology in health fields) governing confidentiality of patients’ information.

The above-mentioned laws/regulations provide for matters related to offences, penalties and enforcement in their respective sphere.

In the UAE, Federal Decree-Law No 45 of 2021 (PDPL) forms the main national data protection law. Alongside this, the DIFC and ADGM have their own data protection regimes that apply within their respective free zones. While separate, these frameworks are broadly aligned with each other and with GDPR principles, reflecting a shared commitment to high standards of personal data protection. The DIFC and ADGM laws also set out more detailed, zone-specific requirements, which are enforced by their own regulatory authorities.

The sector-specific regulations mentioned above regulate the processing of personal data in their respective spheres while complementing the personal data protection laws in the UAE.

1.2 Rights and Obligations

The data privacy laws applicable across the UAE based on the set of principles for the processing of the personal data, which are as follows:

- **Lawfulness:** Personal data must be processed in accordance with applicable legal requirements.
- **Fairness and Transparency:** Processing must be fair to individuals and carried out in a transparent manner.

- **Purpose Limitation:** Personal data must be collected for specified, explicit, and legitimate purposes.
- **Data Adequacy and Relevance:** Personal data must be adequate, relevant, and limited to what is necessary.
- **Data Minimisation:** Only the minimum amount of personal data required for the stated purpose should be processed.
- **Accuracy:** Personal data must be accurate and kept up to date where necessary.
- **Security and Confidentiality:** Appropriate technical and organisational measures must be in place to protect personal data.
- **Storage Limitation/Erasure:** Personal data should not be retained longer than necessary and must be erased or anonymised when no longer required.

Rights of Data Subjects

The following rights are provided to data subjects under the UAE Federal Law, DIFC Law and ADGM Regulations.

- **Right of Access to Information:** A data subject has the right to access his/her processed personal data.
- **Right to Notification:** A data subject has the right to be notified with respect to the processing of his/her personal data.
- **Right to Rectification/Erasure of Personal Data:** A data subject has a right to request the rectification or erasure of their processed personal data.
- **Right to Withdraw Consent:** A data subject has the right to withdraw consent given for the processing of his/her personal data.
- **Right to Restriction/Stopping of Processing:** A data subject has the right to request the restriction or cessation of processing by a controller.
- **Right to Data Portability:** A data subject has the right to receive his or her personal data in a structured and commonly used machine-readable format and to transmit the personal data to another controller.
- **Right Related to Automated Decision-Making and Profiling:** A data subject has the right to not be subjected to a decision solely based on automated decision-making, including profiling.
- **Right to Lodge Complaint:** A data subject has the right to submit a complaint to the relevant data

protection authority if the personal data has been processed in violation of the UAE PDPL, the DIFC Data Protection Law, or the ADGM Data Protection Regulations.

Compliance depends on the nature of the industry, the type of personal data processed, and the quantum of personal data processed. Some examples of compliance mechanisms, which may vary depending on the industry and other factors, are as follows:

- implementing compliance documentation;
- implementing a consent management mechanism;
- implementing a personal data breach procedure;
- facilitating data subjects to exercise their rights;
- implementing appropriate measures to protect personal data; and
- privacy awareness amongst employees in general and capacity building of staff entrusted with privacy compliance.

1.3 Special Categories of Personal Data Federal Decree Law

The Federal Decree Law provides that the controller has an obligation to appoint a Data Protection Officer (DPO) when the controller is involved in the systematic processing and overall assessment of sensitive personal data (special categories of personal data).

Similarly, there is a requirement to carry out a data protection impact assessment when the processing involves a large amount of sensitive personal data.

DIFC Data Protection Law and ADGM Regulations

Special categories of personal data can be processed under the DIFC Law and ADGM Regulations in the following situations:

- when processing is carried out with the explicit consent of the data subject;
- when processing is necessary to fulfil obligations or exercise specific rights of the controller or the data subject in the context of employment;
- when processing is required to protect the vital interests of the data subject;
- when processing is conducted by a foundation, association, or other non-profit organisation as part of its legitimate activities;

- when processing relates to personal data that has been deliberately made public by the data subject;
- when processing is necessary for the establishment, exercise, or defence of legal claims; and
- when processing is required to comply with a specific legal obligation applicable to the controller.

Under the DIFC Law and the ADGM Regulations, criminal convictions are also included in the definition of the special categories of personal data. The Federal Decree Law, DIFC Law and the ADGM Regulations are silent on the matter of the processing of personal data relating to minors.

Federal Decree Law No 26 of 2025 on Child Digital Safety has been enacted to establish a legal framework for safeguarding children in the digital environment. The law aims to protect children from online risks and harmful digital content that may adversely affect their wellbeing, while at the same time ensuring their right to access digital content that is safe, appropriate, and age-appropriate. This law will be implemented after a one-year grace period.

1.4 Processing of Personal Data for Research and Development Purposes

ADGM Regulations

Processing for research purposes is allowed subject to the following conditions, irrespective of the particular circumstances:

- The controller must ensure, through appropriate technical and organisational measures, that personal data, including special categories of personal data, are anonymised and pseudonymised in a way that prevents re-identification. The processing for research purposes must not cause substantial damage to a data subject.
- The processing for research purposes is only allowed if the purpose for processing includes medical research, and it has received the approval of a public authority and research institution.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Through its Regulation 10, the DIFC has enacted amendments to its data protection regulations, aimed at overseeing the use of autonomous and semi-auton-

omous systems, particularly those driven by artificial intelligence (AI) and machines. The regulations apply to AI-driven systems and processes used within the DIFC's jurisdiction – either autonomous systems or semi-autonomous systems. These regulations emphasise:

- the ethical use of systems;
- risk assessment and mitigation;
- accountability and oversight;
- that the processing must be transparent; and
- that users and data subjects must be informed about the role of AI in decisions that affect them.

Although neither the ADGM nor the DIFC has enacted laws specifically dedicated to AI, both have incorporated AI-related considerations into their existing data protection and governance frameworks. These provisions ensure that AI applications in financial services are used responsibly, ethically and in accordance with data protection standards.

1.6 Data Breach Requirement

The data controller, in the event of a personal data breach, is required to notify the relevant competent authority – ie, the Data Office (Federal Decree Law)/Commissioner (DIFC Data Protection Law)/Commissioner of Data Protection (ADGM Regulations), where the breach is likely to pose a risk to the privacy, confidentiality, security, or rights of data subjects. The data processor must notify the controller without undue delay upon becoming aware of such a breach.

Notification timelines differ across UAE jurisdictions:

- Under UAE Federal Law, the breach must be reported immediately.
- Under the DIFC Data Protection Law, notification must be made without undue delay.
- Under the ADGM Data Protection Regulations, notification must be made within 72 hours of becoming aware of the breach. Where notification is not made within this timeframe, the controller must provide reasons for the delay.

The breach notification must include, at a minimum:

- a description of the nature of the breach;

- contact details of the DPO;
- the likely consequences or impact of the breach;
- a description of the measures taken or proposed by the controller to address the breach and mitigate its effects; and
- any additional information required by the UAE Data Office (where applicable under UAE Federal Law).

Where a personal data breach is likely to pose a high risk to the security or rights of a data subject, the controller must also notify the affected data subject of the breach. The notification to the data subject must include the same information that was provided to the competent authority.

1.7 Regulators

The UAE Data Office is the regulator for the purposes of the UAE Law.

The Commissioner administers the DIFC Law while the Commissioner of Data Protection is responsible for the monitoring and enforcement of the ADGM Regulations.

The Central Bank of the UAE and the Telecommunications and Digital Government Regulatory Authority (TDRA) are the regulators concerning the banking and telecommunications sectors, responsible for, among other things, the protection of their respective consumers' data.

Health authorities (federal or local government) are entrusted with the protection of patients' data.

The above-mentioned authorities have the powers of investigation and complaint-handling in their respective spheres.

1.8 Enforcement Proceedings and Fines

The Data Office (concerning the UAE Law) is competent to receive complaints by data subjects regarding contraventions of provisions of the UAE Law. The Data Office is also competent to impose administrative sanctions for contraventions of provisions of the UAE Law. A person aggrieved by any decision, administrative sanction or any action of the Data Office may file a grievance with the Director General of the Data Office.

The grievance is to be filed within 30 days of the date of decision, administrative sanction or action of the Data Office. The Director General of the Data Office is to determine such grievance within 30 days of its filing. The executive regulations to be issued pursuant to the UAE Law will specify the procedural aspects for filing and deciding on such grievances.

The Commissioner of Data Protection (under the DIFC Law) is competent to receive complaints from data subjects concerning contraventions of the DIFC Law or any breach of the rights of data subjects. The Commissioner is empowered to investigate the complaints and to issue a direction or declaration. The Commissioner is empowered to impose fines in the event of non-compliance with a direction issued by them. Concerning a complaint lodged with them, the Commissioner may follow those practices and procedures that will, in the Commissioner's view, lead to the most timely, fair and effective resolution of the claim in the complaint. The controller, processor or data subject aggrieved by the Commissioner's decision may appeal to the DIFC Court within 30 days.

Upon a contravention of the ADGM Regulations, a data subject may lodge a complaint with the Commissioner of Data Protection under the ADGM Regulations. After an assessment, the Commissioner may:

- dismiss the complaint;
- uphold the complaint;
- uphold the complaint but with no further action; or
- take any further action.

The aggrieved controller, processor or data subject may refer the matter to the court for review. The court may make any orders that it thinks just and appropriate in the circumstances, within three months of the penalty notice, direction or date of complaint.

Under the UAE Federal Decree Law, the administrative sanctions to be imposed are issued by the cabinet upon proposal of the Director General of the Data Office.

As per the DIFC Law, when the Commissioner considers that a controller or processor is liable for a contravention of law, they may issue an administrative

fine to the controller or processor. The Commissioner must issue a notice to the controller or processor of the imposition of a fine or may hold the controller or processor liable for damages and compensation payable to the data subject. Administrative fines are set out in Schedule 2 of DIFC Data Protection Law No 5 of 2020. Fines corresponding to the contraventions mentioned in Schedule 2 range from USD10,000 to USD100,000.

Data subjects are also given a private right of action under the DIFC Law, so that when a data subject suffers damage due to a violation of the DIFC Law or its regulations, the data subject may apply to the court for compensation.

Under the ADGM Regulations, if a controller or processor performs an act or abstains from performing an act in contravention of a direction issued by the Commissioner of Data Protection or the ADGM Regulations (or subsequent rules made thereunder), they shall be subject to imposition of an administrative fine by the Commissioner. The Commissioner shall send a written “penalty notice” to the controller or processor. The penalty imposed by the Commissioner must not exceed USD28 million.

1.9 Enforcement Trends

Under the ADGM Regulations the following penalties have been imposed:

- Okadoc Technologies Limited (21 May 2024): The violation involved failure to comply with a data subject’s access request, breaching individual rights. The penalty was a USD20,000 fine under the ADGM Regulations. Adequate processes were lacking for identifying, facilitating and fulfilling the access request.
- VentureRock Global Limited (23 June 2023): The violation involved deficiencies in data security, policies and procedures. The ADGM Commissioner of Data Protection found that poor cybersecurity practices due to human error, inadequate training, and lack of proper policies and procedures contributed to the violation.

Under the DIFC Law, recent amendments have introduced, among other matters, an express principle of

liability and have granted data subjects a private right of action, enabling them to apply to the court for compensation.

2. Privacy Litigation

2.1 Privacy Litigation Overview

As discussed in 2.2 Recent Case Law, the ADGM Commissioner of Data Protection has issued a direction in two different cases with respect to contravention of the ADGM Regulations. However, no active court litigation relating to privacy has arisen in this context.

2.2 Recent Case Law

No court decisions are currently available.

2.3 Collective Redress Mechanisms

UAE law does not provide for collective redress mechanisms for data subjects.

DIFC Law and ADGM Regulations

Under the DIFC Law and the ADGM Regulations, multiple data subjects affected by the same offence or violation may file a collective complaint. In addition, the Commissioner may elect to deal collectively with multiple complaints that relate to the same contravention or breach.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

The TDRA has issued a regulatory policy on the internet of things (IoT). This policy shall be applicable to all persons connected with IoT within the UAE, including but not limited to:

- licensees;
- IoT service providers; and
- IoT service users, including individuals, businesses and the government.

Objective/Scope

The IoT policy encompasses the following objectives:

- ensuring secure IoT services;
- addressing reasonable demands for IoT services;
- promoting continuous innovation in IoT;
- efficiently managing limited resources;
- safeguarding the rights and interests of IoT users; and
- offering transparency to facilitate IoT market growth.

Obligations

Any service provider providing IoT is under an obligation to follow UAE telecommunications laws, regulations and the IoT policy. The IoT service provider has to register with the TDRA and obtain an IoT service provider registration certificate. IoT service providers need to have a local presence or must appoint a representative to have a point of contact with the TDRA.

Service providers must ensure that the service they provide is adequate and reliable. For personal data processing and storage, the IoT service provider must follow the principles of purpose limitation, data minimisation and storage limitation. Secret, sensitive and confidential data of individuals and businesses must be stored within the UAE. However, it can be stored outside the country when such data is afforded adequate or equivalent security. Secret, sensitive and confidential data of the government must remain in the UAE. The service provider has to use encryption standards. Data processors/service providers must establish technical measures to enable the inspection of stored data. IoT services in the UAE are also regulated by Federal Decree Law No 3 of 2023 (the “Telecommunications Law”), under which different penalties apply for contraventions of the law. Defiance of or non-compliance with the IoT policy by IoT service providers or users shall be taken as a breach of the UAE Telecommunications Law, and may be penalised by the TDRA.

There is no law similar or identical to that of the EU Data Act.

3.2 Interaction of Data Regulation and Data Protection

The Federal Law, DIFC Law, and ADGM Regulations recognise the following legal bases for the processing of personal data:

- **Data Subject Consent:** Personal data may be processed when a data subject gives its consent.
- **Performance of Contract:** Personal data may be collected when it is essential for the performance of a contract.
- **Compliance With Legal Obligations:** Personal data may be processed when such processing is necessary for legal compliance purposes.
- **Protection of Vital Interests:** Personal data may be processed when its processing is required for the protection of the vital interests of the data subjects.
- **For Public Tasks:** Personal data processing may be carried out when such processing is essential for the performance of a task vested in a public authority.
- **Legitimate Interests:** Personal data may be processed when the processing is necessary for the legitimate interests of the controller or a third party.

UAE data privacy laws protect the confidentiality of personal data by requiring organisations that collect or use data to put in place proper technical and organisational safeguards. These safeguards are meant to prevent personal data from being accessed, shared, changed, or lost without authorisation. Under the federal Personal Data Protection Law, as well as the DIFC and ADGM frameworks, personal data must be kept secure at all stages of its use, including when it is collected, stored, shared, and eventually deleted.

These laws do not address the IP protection of non-personal data.

3.3 Rights and Obligations Under Applicable Data Regulation

Please see 1.2 Rights and Obligations.

3.4 Regulators and Enforcement

Please see 1.7 Regulators.

4. Sectoral Topics

4.1 Use of Cookies

While there is no specific law regulating the use of cookies in the processing of personal data, existing personal data protection laws apply to their collection and use. Consent must be explicitly obtained from

data subjects before cookies are utilised, and they must be provided with clear and accessible options to opt out of cookie usage.

4.2 Personalised Advertising and Other Online Marketing Practices

The UAE Law confers on the data subject a “right to stop processing” where personal data is processed for direct marketing purposes, including profiling to the extent that profiling is related to such direct marketing.

The DIFC Law provides that a data subject has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing and that the data subject be expressly offered the right to object to direct marketing. The data subject has the right to object to personal data processing for direct marketing purposes, including profiling to the extent profiling is related to such direct marketing.

The ADGM Regulations carry the same provisions as in the DIFC Law, regarding direct marketing. The ADGM Regulations, in addition, provide that when a data subject objects to direct marketing, personal data must not be processed for direct marketing purposes.

4.3 Employment Privacy Law

Federal Decree Law No 33 of 2021, regarding the regulation of employment relationships, provides that a worker should maintain the confidentiality of information and data to which they have access by virtue of their work.

The UAE Law, the DIFC Law and the ADGM Regulations do not contain any provision concerning the role of labour organisations, whistle-blowing or e-discovery.

4.4 Data Protection in M&A

There is no dedicated framework concerning privacy requirements in M&A; instead, the general framework, as discussed elsewhere in this chapter, is applicable.

5. International Considerations

5.1 Restrictions on International Data Transfers

The UAE Law provides that personal data may only be transferred outside the UAE to a jurisdiction with a law in place covering various aspects as to the protection of personal data (ie, an adequate level of protection). Personal data may also be transferred to those countries with whom the UAE has bilateral or multilateral agreements in respect of personal data protection.

Where no adequacy decision exists, the UAE Personal Data Protection Law permits certain transfers of personal data outside the UAE, subject to the Executive Regulation, including the following:

- where legally binding safeguards ensure compliance with UAE data protection standards;
- where the data subject has expressly consented in a manner consistent with public order and national security;
- where the transfer is required for judicial proceedings or the exercise of legal rights;
- where it is necessary to enter into or perform a contract involving or benefiting the data subject;
- where it is undertaken for purposes of international judicial co-operation; or
- where it is justified by public interest considerations.

The DIFC Law provides that personal data may be transferred to a third country or to an international organisation on the basis of an adequate level of protection, as determined by the Commissioner of Data Protection. A list of adequate jurisdictions is issued through the DIFC Data Protection Regulations.

In the absence of an adequate level of protection, the personal data may be transferred by incorporating appropriate safeguards, which may be provided by adopting the following:

- any agreement between public authorities of both the sender and the receiver;
- binding corporate rules;
- standard data protection clauses that will be issued by the Commissioner;

- an approved code of conduct; or
- an approved certification mechanism along with the binding and enforceable commitments of the controller or processor that they will apply appropriate safeguards.

The ADGM Regulations allow the transfer of personal data outside the ADGM or to an international organisation where the Commissioner has decided that the receiving jurisdiction or the international organisation ensures an adequate level of protection.

In addition, in the absence of an adequacy decision, the ADGM Regulations permit cross-border transfers of personal data only where the controller or processor puts in place appropriate safeguards that ensure a comparable level of protection for the data subject.

These safeguards include the use of the following:

- standard contractual clauses or other contractually binding instruments that impose enforceable data protection obligations on the recipient party;
- binding corporate rules for intra-group transfers; and
- approved codes of conduct or certification mechanisms coupled with binding and enforceable commitments by the data recipient.

5.2 Government Notifications and Approvals

There is no requirement for any government notifications or approvals in order to transfer data internationally, except as discussed in **5.3 Data Localisation Requirements** related to health data.

5.3 Data Localisation Requirements

There is no data localisation requirement, except with regard to health information and data, which, under Federal Law No 2 of 2019, may not be stored, processed, generated or transferred outside the UAE, except upon a decision issued by the Health Authority in co-ordination with the Ministry of Health and Prevention.

5.4 Blocking Statutes

There are no blocking statutes in the UAE.

5.5 Recent Developments

No information is publicly available on any changes or anticipated developments concerning the international transfer of personal data.

Trends and Developments

Contributed by:

Nadim Bardawil, Hala Harb and Hebah Innah
BSA LAW

BSA LAW is a leading regional law firm with eight offices across five countries in the Middle East. The firm's diverse team of over 100 lawyers from 35 nationalities, speaking 22 languages, blends global insight with local expertise. As a market leader in TMT, BSA LAW partners with clients at the forefront of innovation, advising on digital transformation, data protection, AI governance and media regulation. More than a traditional law firm, BSA LAW acts as a

strategic collaborator, driving sustainable growth and technological advancement. Founded two decades ago, the firm has grown organically by investing in people and cultivating long-term client relationships. Clients trust BSA LAW for clear, actionable advice and risk management tailored to the rapidly evolving TMT landscape, empowering businesses shaping the future of technology across the Middle East.

Authors



Nadim Bardawil is a partner and head of the TMT and Fintech practices at BSA LAW. He has spent the last decade advising technology, media and fintech companies, including advising on crypto projects for

start-ups and established entities. He regularly assists clients on transactional matters and on navigating local and regional regulatory frameworks. Nadim frequently publishes on TMT topics and speaks at public forums on technology, crypto and fintech. Fluent in English, French and Arabic, he holds a JD from Hofstra University School of Law and is admitted to practice in New York and Dubai.



Hebah Innah is a paralegal in BSA LAW's TMT practice. She supports the team on data protection, cybersecurity, digital platforms and emerging technologies across the GCC. Her work includes drafting and

reviewing data privacy policies, commercial agreements and platform terms. Hebah conducts legal research on AI, blockchain, fintech and e-commerce regulation.



Hala Harb is a senior associate in the TMT practice at BSA LAW, specialising in data privacy, fintech, telecom regulatory compliance and technology agreements. With experience in private practice and

in-house roles, she provides tailored counsel that prioritises clients' strategic goals, risk management and business needs. Hala offers regulatory guidance in tech, fintech and telecom sectors, ensuring compliance with evolving regulations. She advises clients in regulated industries such as finance and health on data privacy, applying GDPR-comparative approaches. Prior to BSA LAW, Hala served as in-house counsel at a leading Dubai media company and for the digital platforms of a prominent news channel.

BSA LAW

Level 6
Building 3
Dubai International Financial Centre (DIFC)
The Gate District
PO Box 262
Dubai
United Arab Emirates

Tel: +971 452 855 55
Email: info@bsalaw.com
Web: bsalaw.com



An Evolving Privacy Landscape

The UAE has been steadily building out its data protection framework, and the most significant developments have come from the financial free zones, DIFC and ADGM.

For businesses operating in or from the UAE, compliance is rarely a matter of following a single set of rules. Organisations typically need to navigate overlapping obligations that shift depending on where they are based, what sector they operate in, and how personal data flows between the mainland and the free zones. In this article, we will walk through the current state of the UAE's data protection landscape, draw out the key differences between the mainland and free zone regimes, and outline the practical compliance risks that surface in the absence of a fully harmonised enforcement framework.

UAE Mainland Data Protection Law and Enforcement

The UAE's onshore data protection framework is anchored by Federal Decree-Law No 45 of 2021 on the Protection of Personal Data (PDPL). It applies broadly to the processing of personal data of individuals residing in the UAE, with limited exemptions, and can extend beyond UAE borders in certain circumstances. One important carve-out: entities in the DIFC and ADGM are expressly excluded, as they operate under their own standalone data protection regimes.

Despite its broad scope, the PDPL is still very much a work in progress. The Implementing Regulations, intended to clarify key aspects of the law, have yet to be issued. The practical effect has been limited enforcement activity and a cautious regulatory stance, with most organisations driving their own compliance through internal risk assessments rather than in response to regulatory action.

On the supervisory side, Federal Decree-Law No 44 of 2021 established the Emirates Data Office as the primary authority responsible for overseeing data protection on the mainland. However, the Data Office has not yet become fully operational. The law provides that, during its initial two-year transitional period, the Telecommunications Regulatory Authority (TDRA) and the Digital Government are to provide administrative and logistical support. In practice, the TDRA has been observed to act as a point of contact for data protection-related inquiries.

Parallel Data Protection Obligations Under Other Laws in the UAE

The fact that the PDPL has yet to be fully operationalised does not, in itself, reduce the scope of data protection obligations that organisations in the UAE must already satisfy. Notwithstanding the PDPL's limited enforceability to date, a number of sector-specific laws and regulations already impose binding data protection and confidentiality obligations across the UAE. Taken together, these instruments establish that robust data protection compliance is already a

legal necessity, not a matter to be deferred pending full operationalisation of the PDPL.

The Cybercrime Law (Federal Decree Law No 34/2021) represents perhaps the broadest existing framework. It criminalises the unauthorised access, collection, processing, disclosure, or misuse of personal data through information technology systems, with enhanced penalties where the data in question relates to sensitive categories, including medical records, banking information, or electronic payment data. The unauthorised disclosure of confidential information obtained through employment or a professional capacity also constitutes an offence under this law.

In the public sector, the Information Security Resolution (Cabinet Resolution No 21 of 2013) imposes mandatory information security obligations on federal government entities, requiring the protection of personal and confidential data through measures including access controls, encryption, data classification, and restrictions on external storage.

Within the telecommunications sector, the TRA Consumer Policy requires service providers to limit the processing of subscriber data to purposes directly related to the provision of telecom services. Prior consent must be obtained before personal information is shared with affiliates or third parties, and consumers are afforded the right to access their data and to prevent its unauthorised disclosure.

Under the Healthcare ICT Law (Federal Law No 2 of 2019), health information must be maintained in confidence, stored within the UAE absent specific regulatory approval, and used exclusively for health-related purposes. These requirements are further reinforced within Dubai Healthcare City by the DHCA Health Data Protection Regulation No 7 of 2013, which establishes a comprehensive regime governing the collection, use, storage, disclosure, transfer, and retention of patient health information.

Licensed financial institutions operating under the CBUAE Consumer Protection Regulation and Standards are similarly required to protect consumers' personal and financial data through confidentiality meas-

ures and appropriate security safeguards, to disclose the basis on which personal data is collected and used, and to prevent unauthorised access or excessive processing.

The Penal Code (Federal Law 21 of 2021) further reinforces the criminal dimension of data protection in the UAE. Under Article 431, it is an offence to intercept or eavesdrop on a private conversation, or to capture or transmit images of a person obtained in a private setting, in each case in the absence of the data subject's consent.

Taken together, these provisions make clear that organisations operating in the UAE are already subject to a substantive body of binding data protection obligations.

DIFC: Enhanced Enforcement and Private Rights of Action

Data protection in the DIFC is governed by the Data Protection Law, DIFC Law No 5 of 2020 (the "DIFC DP Law"), which sets out a comprehensive framework regulating the collection, handling, and use of personal data, together with enforceable rights and remedies for individuals. What sets the DIFC apart, however, is not just the framework itself. It is the pace and ambition with which it is evolving.

The DIFC has demonstrated a clear appetite for keeping its regulatory infrastructure ahead of technological change. Perhaps the most notable example is Regulation 10, enacted in September 2023, which places the DIFC among the first subnational jurisdictions globally to specifically regulate AI and autonomous systems in the context of personal data processing. Regulation 10 places the burden of compliance squarely on "deployers" and "operators", the entities that authorise or benefit from AI systems, requiring them to ensure that personal data is processed transparently, fairly, and ethically, with clear accountability built into the design of these systems. This proves DIFC's efforts to ensure that the data protection regulations are evolving alongside the ever-changing technology.

In July 2025, amendments to the DIFC DP Law materially strengthened the enforcement landscape in ways that have direct practical implications for organisa-

tions. Most significantly, data subjects can now bring claims directly before the DIFC courts without first needing to engage the DIFC Commissioner of Data Protection, a procedural requirement that had, in practice, acted as a barrier to litigation.

The territorial reach of the DIFC DP Law has also been clarified. It now applies not only to entities incorporated in the DIFC, but to any controller or processor, including those based outside the DIFC, that processes personal data of individuals residing or working there, whether directly or through third-party arrangements.

Separately, the rules around sharing personal data with third-country authorities have been tightened, with controllers now required to verify that any such request is valid and proportionate before any disclosure is made. Taken together, these changes reflect a regulatory environment that is deliberately designed to stay ahead of, rather than simply respond to, the challenges that organisations face.

ADGM: Targeted Reforms and Substantial Public Interest Processing

Data protection in the ADGM is governed by the ADGM Data Protection Regulations 2021 (the “ADGM DP Regulations”). In September 2025, the ADGM Registration Authority introduced the Data Protection Regulations (Substantial Public Interest Conditions) Rules 2025 (the “ADGM Rules”), a focused refinement addressing a practical gap in the existing framework.

While consent remains the default basis for processing special categories of personal data, including health, biometric, and genetic data, there are circumstances in which obtaining it is neither possible nor appropriate. The ADGM Rules draw the boundaries of those circumstances with care, concentrating on two areas where the tension between data protection and broader public interest is most acute: insurance and the safeguarding of vulnerable individuals.

In the insurance context, the ADGM Rules permit the processing of sensitive personal data where it is necessary for underwriting, policy administration, claims handling, or compliance with legal obligations. Where the processing does not directly concern the individ-

ual, the controller must demonstrate that obtaining consent was not reasonably practicable and that the individual has not actively refused it. Notably, silence does not constitute refusal. This enables insurers to act promptly where needed, while preserving consent as the default position.

The safeguarding provisions operate on a similar basis but in a context where the stakes are higher. Sensitive data may be processed without consent for the purpose of protecting children and vulnerable adults who are unable to safeguard themselves, particularly where seeking consent would itself place the individual at greater risk. This provides the necessary legal basis for timely disclosures to relevant authorities in cases of neglect, abuse, or exploitation.

Cross-Border Transfers From the Mainland and Best Practice in the Absence of Formal Mechanisms

Businesses operating in or from the UAE are frequently subject to multiple and overlapping data protection regimes, depending on their place of establishment, the location of customers or employees, and the structure of their operations. For many organisations, particularly those with group entities spanning the mainland and financial free zones, effective compliance requires a jurisdiction-sensitive approach, rather than reliance on a single, uniform framework.

In practice, organisations often overlook that the transfer of personal data between the UAE mainland and financial free zones such as the DIFC and ADGM (and vice versa) is treated as a cross-border data transfer, notwithstanding that all jurisdictions are located within the UAE. This is because the mainland, DIFC, and ADGM operate as separate legal jurisdictions with distinct data protection regimes. As a result, transfers from the mainland to the DIFC or ADGM must satisfy the cross-border transfer requirements of the receiving jurisdiction’s data protection law, and may trigger transfer assessments, contractual safeguards, or regulatory scrutiny, particularly where regulated or sensitive data is involved.

While the PDPL does contemplate mechanisms for managing such transfers, the Implementing Regulations necessary to give full effect to these provisions

have yet to be issued. In the absence of fully operational federal transfer mechanisms, many organisations and multinational groups have adopted risk-based compliance approaches, commonly grounded in contractual safeguards aligned with GDPR-style standards. These typically include data transfer and processing agreements with enhanced confidentiality and security obligations, commitments to apply equivalent data protection standards in recipient jurisdictions, and internal policies governing data access, retention, and onward transfers. While not yet formally enforced under the PDPL, such measures are widely regarded as best practice and are likely to be viewed favourably by regulators as enforcement activity matures.

Conclusion

The UAE's data protection regime is best understood not as a single, unified framework, but as a composite system of federal, free zone, and sector-specific obligations, each operating at a different stage of regulatory maturity.

For organisations operating across the mainland and the free zones, navigating this landscape requires more than a cursory read of the relevant statutes. It demands a jurisdiction-aware, risk-based approach, particularly when it comes to intra-UAE data transfers, which are far more legally complex than they might first appear.

In the current environment, where enforcement is still developing but obligations are already binding, organisations cannot afford to take a wait-and-see approach.

Contractual safeguards, robust internal governance, and alignment with international best practices are no longer optional; they are practical necessities for managing regulatory exposure. As enforcement activity inevitably increases and institutional capacity continues to mature, organisations that have already put these measures in place will be meaningfully better positioned to meet heightened scrutiny and evolving expectations.



Law and Practice

Contributed by:

Aly Dossa and Marcus Burnside
Chamberlain Hrdlicka

Contents

1. Legal and Regulatory Framework p.545

- 1.1 Overview of Data and Privacy-Related Laws p.545
- 1.2 Rights and Obligations p.547
- 1.3 Special Categories of Personal Data p.548
- 1.4 Processing of Personal Data for Research and Development Purposes p.548
- 1.5 Processing of Personal Data in the Context of Artificial Intelligence p.549
- 1.6 Data Breach Requirement p.549
- 1.7 Regulators p.550
- 1.8 Enforcement Proceedings and Fines p.550
- 1.9 Enforcement Trends p.551

2. Privacy Litigation p.551

- 2.1 Privacy Litigation Overview p.551
- 2.2 Recent Case Law p.551
- 2.3 Collective Redress Mechanisms p.552

3. Requirements for the Protection and Processing of Non-Personal Data p.552

- 3.1 Objectives and Scope of Data Regulation p.552
- 3.2 Interaction of Data Regulation and Data Protection p.552
- 3.3 Rights and Obligations Under Applicable Data Regulation p.552
- 3.4 Regulators and Enforcement p.553

4. Sectoral Topics p.553

- 4.1 Use of Cookies p.553
- 4.2 Personalised Advertising and Other Online Marketing Practices p.554
- 4.3 Employment Privacy Law p.555
- 4.4 Data Protection in M&A p.556

5. International Considerations p.556

- 5.1 Restrictions on International Data Transfers p.556
- 5.2 Government Notifications and Approvals p.557
- 5.3 Data Localisation Requirements p.557
- 5.4 Blocking Statutes p.558
- 5.5 Recent Developments p.559

Chamberlain Hrdlicka is a nationally recognised law firm offering a full suite of legal services to businesses and individuals across a wide range of industries. With offices in Houston, Atlanta, Philadelphia and San Antonio, it combines the experience of a large firm with the personal attention of a boutique practice. In respect of data security and privacy, the firm understands how data is captured, stored, transferred and monetised, with experience spanning Fortune 100 companies, leading internet firms, communications providers, mid-size businesses and emerging start-

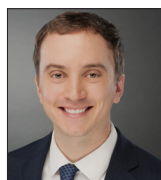
ups. It is well-versed in legal issues and possesses deep technical knowledge of data flows, system interfaces and technology implementation. It navigates complex federal and state laws, each requiring immediate, compliant breach responses and subsequent obligations. Leveraging its comprehensive, multidisciplinary legal and industry experience, it identifies trends and anticipates risks across industries, providing forward-thinking, customised legal strategies to help clients succeed.

Authors



Aly Dossa is intellectual property and technology practice group chair at Chamberlain Hrdlicka. For over 23 years, he has focused on intellectual property counselling and litigation for software, hardware, medical device

and consumer device companies, from start-ups to Fortune 100 firms. Aly helps clients navigate the dynamic regulatory landscape, advising on data privacy, cross-border transfers, compliance, breach response and M&A due diligence. He develops global IP strategies, handles patent and trade mark prosecution, negotiates licences and provides legal opinions. He holds certifications as a Certified Information Privacy Professional (CIPP/US), Certified Information Privacy Manager (CIPM), and Artificial Intelligence Governance Professional (AIGP) through IAPP.



Marcus Burnside is senior counsel at Chamberlain Hrdlicka. He focuses his practice on intellectual property for domestic and foreign clients. With mechanical and electrical engineering knowledge, he assists clients across

technologies including computer hardware, oil and gas, automation, robotics, communication systems, data storage and green energy. Marcus drafts patent applications, office action responses and appeal briefs. He counsels on IP matters including licence negotiation, non-infringement and invalidity opinions, and due diligence. His practice supports AI companies with strategic IP protection, machine learning data procurement, AI integration and regulatory compliance. Marcus holds certifications as a Certified Information Privacy Professional (CIPP/US) and Artificial Intelligence Governance Professional (AIGP) through IAPP.

Chamberlain Hrdlicka

1200 Smith Street
Suite 1400
Houston, TX 77002
USA

Tel: +1 713 654 9672
Fax: +1 713 658 2553
Email: aly.dossa@chamberlainlaw.com
Web: www.chamberlainlaw.com



1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Constitutional Foundations

The US Constitution does not explicitly guarantee a right to privacy, but courts have recognised certain privacy protections through constitutional interpretation. The Fourth Amendment protects against unreasonable searches and seizures, establishing limits on government surveillance and data collection. Various Supreme Court decisions have recognised implicit privacy rights in specific contexts; however, these rights do not apply to non-governmental actions.

Statutory Framework

The United States lacks a comprehensive federal data privacy law comparable to the Europe's GDPR. Instead, privacy and data laws operate through a combination of state and federal laws. In this patchwork, the federal laws operate through a domain-specific approach that applies to certain data types being used within certain contexts. Meanwhile, some states have enacted general data privacy laws and additional domain-specific laws, but these state laws often have exemptions for data protected by particular federal laws. While many of these laws are less onerous than GDPR, the fractured approach requires a broader base of knowledge, both from legal and technical perspectives.

Federal Laws

The following provides a list of the most commonly applicable federal laws that apply to data and privacy. However, it should be appreciated that there are several, rarely applicable laws (including ones that have never been enforced).

- Health Insurance Portability and Accountability Act (HIPAA) – governs the use and disclosure of protected health information by covered entities and their business associates.
- Gramm-Leach-Bliley Act (GLBA) – regulates financial institutions' collection, use and disclosure of consumers' personal financial information.
- Children's Online Privacy Protection Act (COPPA) – requires parental consent for collection of personal information from children under 13. An

updated version of COPPA, known as COPPA 2.0, is currently working through Congress and may be passed this year.

- Family Educational Rights and Privacy Act (FERPA) – protects the privacy of student education records.
- Fair Credit Reporting Act (FCRA) – regulates the collection, dissemination and use of consumer credit information.
- Electronic Communications Privacy Act (ECPA) – governs law enforcement access to electronic communications and associated data.
- Video Privacy Protection Act (VPPA) – restricts disclosure of personally identifiable rental records for video materials.
- Cable Communications Policy Act – protects subscriber privacy for cable television services.
- Telephone Consumer Protection Act (TCPA) – restricts telemarketing calls, auto-dialed calls and text messages.
- CAN-SPAM Act – establishes requirements for commercial email messages.
- Genetic Information Nondiscrimination Act (GINA) – prohibits discrimination based on genetic information in health insurance and employment.

Enforcement of these laws is distributed across different federal agencies, and, in some cases, enforcement can be deferred to state attorneys general.

In addition to the above laws that specifically address data privacy, other federal laws can be used to enforce data collection and use. The most prominent of these laws is The Federal Trade Commission Act that empowers the FTC to bring enforcement actions against unfair or deceptive trade practices, which has become a significant source of privacy regulation through enforcement actions and consent decrees.

State-Level Comprehensive Privacy Laws

19 states have enacted comprehensive consumer privacy laws as of early 2026, with more legislation pending. Each state law contains different obligations, exemptions, scope provisions and enforcement mechanisms. Notable examples include:

- Texas Data Privacy and Security Act (TDPSA);

- California's Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA);
- Virginia's Consumer Data Protection Act (VCPA);
- Colorado Privacy Act;
- Connecticut Data Privacy Act; and
- Utah Consumer Privacy Act.

These laws generally share common features including consumer rights (access, deletion, correction, portability), business obligations (transparency, purpose limitation, data security) and opt-out rights for certain data uses, but differ significantly in their thresholds for applicability, definitions, exemptions, private rights of action and enforcement authority.

Between 30–35 states have enacted more limited sectoral privacy laws addressing specific technologies or data types, such as biometric data, genetic information, insurance data or financial data.

In addition, many states have older laws that did not contemplate data collection but are now being applied to data collection practices. The most notable type of these laws is recording consent laws that were originally intended to apply to the recording of phone calls, but have now been applied to online interactions, and most notably to data collection on websites.

Interaction Between Federal and State Laws

Federal sectoral laws generally pre-empt conflicting state laws within their specific domains. For example, HIPAA pre-empts state health privacy laws that provide less stringent protections but allows states to maintain more protective standards. GLBA similarly pre-empts state financial privacy laws to a significant extent.

State comprehensive privacy laws typically contain exemptions for data and entities already regulated under federal sectoral laws, creating a complex patchwork where different rules apply depending on the type of data, the entity collecting it, the context of collection and the use of the data. Organisations handling multiple data types must comply with overlapping federal sectoral requirements, state comprehensive laws and additional state-specific sectoral requirements.

This fragmented approach creates significant compliance complexity, as organisations must navigate which law applies to which data processing activity, with potential gaps where certain data or activities fall outside all regulatory frameworks.

Extraterritorial Reach

Several state privacy laws have extraterritorial application. California's CCPA/CPRA applies to businesses that collect personal information of California residents, regardless of where the business is located, if the business meets certain revenue or data processing thresholds. Similarly, Virginia, Colorado, Connecticut and other states apply their laws to controllers and processors that conduct business in the state or produce products or services targeted to state residents.

These extraterritorial provisions are triggered by factors such as targeting residents of the state, conducting business in the state or meeting quantitative thresholds related to the number of residents whose data is processed. The various state laws use different threshold tests, creating additional complexity for multi-state operations.

Federal sectoral laws generally apply based on the nature of the regulated entity or activity rather than geographic considerations, though they apply throughout US jurisdictions.

Interplay With Non-Personal Data, Cybersecurity and AI Regulation

Cybersecurity

The distinction between privacy and cybersecurity regulation is often blurred. All 50 states have enacted data breach notification laws with varying requirements for timing, content and triggers. Federal sectoral laws like HIPAA and GLBA include security requirements alongside privacy provisions. The Cybersecurity and Infrastructure Security Agency (CISA) plays a role in critical infrastructure protection, which also have additional cybersecurity requirements. Several states have enacted cybersecurity frameworks requiring reasonable security measures, with some specifically addressing ransomware and incident response.

Non-personal data

US law focuses primarily on personally identifiable information, with less regulation of anonymised or aggregate data. However, the boundaries are increasingly contested as re-identification techniques improve (ie, using a collection of non-identifying data to identify an individual). State privacy laws vary in how they define personal information and whether they regulate pseudonymised or de-identified data. Trade secret and intellectual property laws may govern certain business data.

AI regulation

AI-specific privacy regulation is emerging but remains limited. The federal government continues to change and evolve its stance on AI use and regulation but has largely used existing laws and regulations to enforce AI-related use. Colorado has enacted requirements for high-risk AI systems. Several states have proposed AI-specific legislation addressing algorithmic discrimination, automated decision-making, and transparency. Federal sectoral regulators (FTC, EEOC, CFPB) have issued guidance on AI applications within their domains. The interplay typically involves applying existing privacy principles (transparency, fairness, purpose limitation) to AI-driven processing, with questions about whether automated decision-making requires heightened protections.

Regulatory enforcement and trends

Enforcement authority varies significantly. Federal laws are typically enforced by designated agencies (FTC, HHS, FCC, etc). State comprehensive privacy laws grant enforcement authority to state attorneys general. However, some states provide a limited private right of action under certain statutes. This creates a multi-regulator environment where various authorities may have overlapping jurisdiction.

The trend is toward increased state-level activity given federal legislative gridlock; however, both state and federal enforcement has adjusted to view data privacy as a subset of consumer protection. Meanwhile, the plaintiff's bar continues to use older laws applied to new technologies to drive compliance in highly specific domains or use cases of data.

1.2 Rights and Obligations

General Principles for Processing Personal Data

As discussed in **1.1 Overview of Data and Privacy-Related Laws**, US privacy laws operate through a complex patchwork that have been enacted across decades and meant to accomplish divergent goals. Despite this complexity, a common theme throughout most US privacy laws is that organisations should provide clarity. As such, there is very limited ability to provide generally applicable guidance on rights and obligations for personal data. Instead, the following serves as a framework for the practical steps of achieving compliance with US privacy laws.

Practical Implementation Checklist

Organisations should approach compliance in phases.

- Assessment phase – determine applicable laws, conduct gap analysis, identify high-risk activities and prioritise based on legal risk and enforcement patterns.
- Foundation phase – create data inventory, map data flows, inventory systems and vendors, and establish data governance.
- Operational phase – draft policies, implement rights management systems, configure consent mechanisms, execute vendor contracts, deploy security controls and establish training programmes.
- Ongoing phase – monitor regulatory developments, conduct periodic compliance reviews, update processes as business changes, and maintain records of requests, assessments and compliance decisions.

Critical elements vary by applicable law. Examples of some of the most commonly applicable privacy laws include:

- HIPAA requires designated officers, workforce sanctions, Business Associate Agreements and Security Rule safeguards;
- COPPA requires age-screening, verifiable parental consent and limited collection;
- GLBA requires annual privacy notices, opt-out mechanisms and information security programmes; and

- state comprehensive privacy laws often require “Do Not Sell” links, universal opt-out signal recognition, data protection assessments and authenticated consumer portals in some jurisdictions.

Organisations should prioritise compliance efforts based on legal risk (laws with private rights of action or active enforcement), data sensitivity (health, financial, biometric, children’s data), scale of processing, reputational exposure and business criticality, recognising that compliance is an ongoing process requiring continuous monitoring and adaptation.

1.3 Special Categories of Personal Data

Because US federal law addresses special categories of data primarily through sectoral regulation rather than comprehensive frameworks, each category of data governed by a federal law could be considered a special category. Some example statutes are provided in **1.1 Overview of Data and Privacy-Related Laws**.

At the state level, state comprehensive privacy laws typically classify as “sensitive personal information” requiring enhanced protections: health data, biometric data (with approximately 15 states having specific biometric privacy statutes requiring informed consent), genetic information, precise geolocation data, citizenship or immigration status, data revealing racial or ethnic origin, religious beliefs, sexual orientation, social security numbers, financial account credentials, and in some states, union membership or communications content.

Processing sensitive data under state laws generally requires either affirmative opt-in consent or at minimum providing consumers with the right to opt out of such processing, along with heightened security measures, purpose limitations and more stringent vendor oversight. Several states prohibit processing that results in unlawful discrimination based on protected characteristics and restrict certain automated decision-making using sensitive categories.

Data Relating to Minors and Criminal Convictions

COPPA applies to operators of websites or online services directed to children under 13, or operators with actual knowledge they are collecting personal information from children under 13, requiring operators to

post clear privacy policies, provide direct notice to parents, obtain verifiable parental consent before collecting information, honour parental rights to review and delete children’s information, maintain confidentiality and security of children’s data, and limit collection to what is reasonably necessary for participation in the activity.

Some state laws extend protections beyond age 13, with California’s Age-Appropriate Design Code Act (currently subject to litigation) imposing obligations for likely child users under 18, and several states enacting restrictions on social media platforms’ use of minors’ data for targeted advertising or requiring parental consent for minors’ accounts.

Regarding criminal conviction data, FCRA restricts consumer reporting agencies from including arrests over seven years old, paid tax liens over seven years old, and most other adverse information over seven years old in consumer reports, while the Equal Employment Opportunity Commission (EEOC) provides guidance limiting employers’ use of arrest and conviction records to avoid discriminatory impact under Title VII.

State comprehensive privacy laws generally do not create special categories for criminal history data separate from general personal information protections, though state-specific “ban the box” laws, fair chance hiring statutes, and criminal record sealing/expungement laws limit when and how employers, landlords and others may request, consider or retain criminal history information.

1.4 Processing of Personal Data for Research and Development Purposes

Anonymisation for Product Development and Scientific Research

The first step is to determine which laws apply to the data. In the US, HIPAA commonly applies to personal health information (PHI), but there are many circumstances under which HIPAA does not apply to PHI, and other laws, including various federal and state laws, may apply. In addition, there are different exemptions for the use of PHI for research purposes under most privacy laws. Further, anonymising or de-identifying can cause PHI to no longer be considered PHI under US laws, and thus the various laws gov-

erning PHI would not apply. However, as described above, advances in technology can make de-identified data become identifiable data. Thus, even if data is not governed by current laws and the laws do not change, technology changes can cause some of these laws to start applying, causing de-identification to be a moving target requiring ongoing compliance review.

Impact of Health Data Space Regulations

Unlike the European Union's Health Data Space Regulation, which creates a comprehensive framework for secondary use of health data for research, innovation and policymaking with centralised data access bodies and standardised procedures, the United States has no comparable federal initiative establishing a unified health data infrastructure or streamlined access mechanisms for research and product development. The absence of a centralised health data access framework means companies must negotiate individual data use agreements with healthcare systems, navigate varying institutional policies, address inconsistent state law requirements across jurisdictions, and manage complex consent requirements when combining data from multiple sources, thus creating significantly higher transaction costs and longer timelines compared to the streamlined mechanisms envisioned in European health data space initiatives, though potentially offering greater flexibility in commercial applications once data access is secured. Further, as with any other data type, US-based organisations should ensure that any data originating from Europe is obtained and used in a manner that is in compliance with European data privacy laws.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

AI-Specific Requirements and Guidance

The US lacks comprehensive federal AI legislation comparable to the EU AI Act, and instead largely relies on the application of existing laws to AI usage. One complication that arises from this is that users of AI systems often cannot specify what caused an AI tool to create the output that it created. One common issue is the use of AI tools in decision-making where a protected class (eg, race, religion, national origin, etc) could affect a decision, such as hiring. This creates an extra oversight step when implementing an AI tool because these tools can use secondary information to

infer protected class information and generate outputs on that basis.

Several states have introduced legislation specifically governing the use of AI, particularly in relation to decisions that are considered significant life decisions, such as hiring, financial decisions, legal decisions, etc. However, the trend in the US is that regulators are relying on the application of existing laws to AI usage to avoid over-regulating the usage of AI.

1.6 Data Breach Requirement

Notification Requirements

All 50 states have enacted data breach notification laws with varying requirements for timing, triggers, content and scope, creating a complex patchwork that organisations must navigate following a security incident. Generally, organisations must provide notice to affected individuals when there has been unauthorised acquisition of computerised personal information that compromises the security, confidentiality or integrity of the information and creates a risk of harm.

Federal sectoral laws impose additional requirements: HIPAA requires covered entities and business associates to notify affected individuals within 60 days of breach discovery, notify HHS within 60 days (for breaches affecting 500+ individuals, immediate notice; for smaller breaches, annual reporting), and notify media for breaches affecting 500+ individuals in a state or jurisdiction. GLBA requires financial institutions to notify customers as soon as possible when sensitive customer information has been misused, with notification to primary federal regulators. The FTC has authority to bring enforcement actions against organisations that fail to provide reasonable security or that make deceptive statements about their security practices, even absent specific breach notification violations.

Organisational Action Items and Authority Investigations

Prior to any data breach, organisations should obtain cyber insurance so that breach response resources will be made very quickly available, at controlled costs, and using vendors pre-approved by their insurance. Regardless of whether an organisation has cyber

insurance, upon discovering a potential data breach, organisations should:

- immediately activate incident response plans and assemble response teams (legal, IT, security, communications, executive leadership);
- contain the incident and preserve evidence for forensic investigation;
- engage in communications with a threat actor using a threat actor communications expert;
- conduct preliminary assessment to determine scope, nature and cause of the breach;
- assess what personal data was accessed or acquired and which individuals are affected; and
- evaluate risk of harm to individuals considering data sensitivity, likelihood of misuse and any actual misuse.

There are many other additional actions that will likely need to be taken depending on the details surrounding the incident, including, for example, the type of incident, type of data implicated, which laws are applicable, etc.

Often, in the wake of an incident, competent authorities including state attorneys general, the FTC, HHS Office for Civil Rights, state regulators and sector-specific federal regulators initiate investigations based on breach notifications, consumer complaints or their own monitoring. Further, as information about the incident is made public, often following the required notifications, mass data privacy litigation follows, with plaintiffs filing class actions alleging negligence, breach of contract, breach of implied contract, unjust enrichment, violations of state consumer protection statutes and violations of state data breach notification laws, though standing requirements and damages theories remain contested and are addressed in detail in **2. Privacy Litigation**.

1.7 Regulators Investigations

The specific regulator having jurisdiction over investigations is highly fact specific and can include a number of different federal agencies, state agencies and state attorneys general. However, regardless of the regulator, the investigation workflow is largely the same. Generally, the regulating authorities have moni-

tors in place to identify organisations which have suffered an incident and will do a preliminary fact-finding action to determine the scope and severity of the incident, which may be based on their own research (eg, of activity on the dark web), notifications made directly to them, notifications made to affected individuals, complaints from the general public, or from other regulators who may not have jurisdiction, but did discover the incident.

In most instances, an incident will give rise to overlapping jurisdiction amongst the regulators. This gives the regulators, who are often resource constrained, the ability to work together to allocate those resources. As such, many incident investigations are conducted by a consortium of regulators.

Guidance

Regulators often give guidance on privacy issues under their jurisdiction. Whether this guidance is binding depends on the regulator and through which mechanism the guidance was provided. This guidance often provides “safe harbour” rules in terms of which, if followed, the regulator will not pursue any actions. Further, regardless of the enforceability of the guidance, it can provide insight into what that particular regulator reviews when making enforcement decisions.

1.8 Enforcement Proceedings and Fines Investigation and Enforcement Procedures

Data privacy investigations in the US are initiated and conducted by multiple authorities with varying procedures depending on jurisdiction and applicable law. Enforcement proceedings vary greatly based on the regulator bringing the enforcement action. Most enforcements are resolved as the result of an agreement made between a regulator and the affected organisation.

However, if no agreement is reached, the resulting actions differ between federal enforcement and state enforcement. At the federal level, most federal agencies have procedures internal to the agency to handle enforcement actions, causing federal court actions to be rare and arise only when an organisation appeals a decision made within the agency or if the agency refers a case to the Department of Justice. At the

state level, there are fewer agency bodies available and most actions are taken in lawsuits between the state and the affected organisation.

Due to the patchwork framework of the US, the procedural rules vary greatly based on which regulator is initiating an action. However, privacy laws are usually civil in nature, and thus these actions usually align with the local procedural rules. In addition, the penalties vary greatly by regulator, and review of a particular regulator is required to better understand what types of penalties are enacted, often including an agreement to remedy prior violations, take actions to prevent future harm, make recurring disclosures to regulators and payment of fines.

1.9 Enforcement Trends

Significant Enforcement Actions (2023-2025)

Recent enforcement activity has intensified and monetary damages have significantly increased. The FTC has aggressively pursued cases involving health and children's data, including a USD10 million proposed settlement with Disney over COPPA violations, settlements with Cerebral (USD7 million) and GoodRx (USD1.5 million) for issues affecting health information with advertising platforms, and actions against Rite Aid for using facial recognition technology without adequate safeguards and accuracy testing. Biometric privacy enforcement has intensified under state laws, with BNSF settling a class action litigation under Illinois' Biometric Information Privacy Act (BIPA) for USD75 million. State attorneys general have increased co-ordinated multi-state investigations and enforcement, with major actions including a USD391.5 million settlement with Google (40 states) for deceptive location-tracking practices. In addition, Texas has emerged as one of the strictest enforcers with the Texas Attorney General securing a USD1.4 billion settlement with Meta in 2024 and a USD1.375 billion settlement with Google, each for unlawful capture and use of biometric data through facial recognition features without proper consent.

Emerging Trends

In the past, US privacy law enforcement was largely left to federal agencies tasked with their domain-specific enforcement. However, recently, state level enforcement, beginning with California, and reaching

new highs in Texas, has significantly increased the breadth and scope of enforcement in the US. In addition, many of these regulators are seeking more onerous operational penalties on organisations, restricting types of data they can collect and what they can do with certain data that exceed the statutory requirements.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Dispute Trends

Litigation between private parties most often results from a data breach, which, as discussed in **1.6 Data Breach Requirement**, includes plaintiffs filing class actions alleging negligence, breach of contract, breach of implied contract, unjust enrichment, violations of state consumer protection statutes and violations of state data breach notification laws. Other common lawsuits include: actions under the California Invasion of Privacy Act (CIPA) resulting from the use of certain online tracking tools on websites; and lawsuits in response to a Business Email Compromise (BEC) in which an attacker gains access to an email account and tricks customers or employees into sending money or sensitive information, often by changing payment details or sending fake invoices.

The potential damage model for each dispute is highly dependent on the underlying law and facts. For example, in a class action lawsuit resulting from a data breach, the damages are often a relatively small amount per person, but that amount is multiplied potentially millions of times, creating significant risk. In contrast, laws like CIPA provide statutory damages (ie, a set amount of damages per violation), which can also be multiplied many times to create significant risk. Further, suits based on a BEC are dependent solely on the amount of money wrongly sent.

2.2 Recent Case Law

The patchwork system of the US means that the case law is highly specific to the particular governing law. In addition, most actions, particularly those brought by regulators, are settled before a case is even filed. As such, there is often a small body of case law, and

review of the enforcement actions and trends of a regulator is required.

For state-level actions, there exists some case law but, due to the recent nature of these cases, many of them have not advanced far enough through the court systems to become precedential. For example, most CIPA litigation has not reached an appeals court that can release precedential opinions and, as such, the current case law is viewed more similar to enforcement trends rather than precedential case law.

2.3 Collective Redress Mechanisms

In the US, collective redress mechanisms are referred to as class action lawsuits, which have been discussed above. These lawsuits often last years and are commonly settled after key decisions are made by the presiding judge.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

The United States does not have an overarching federal framework comparable to the EU Data Act for governing non-personal data or mandating cross-sector data access. Instead, US law relies on a patchwork of federal and state laws that prioritise cybersecurity, consumer protection and national security concerns over structured data-sharing rights. As a result, companies do not have statutory entitlements to access or reuse non-personal data; these arrangements are left largely to private contract.

Federal statutes such as the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act protect systems and communications against unauthorised access (including access to non-personal data); these statutes do not address any form of lawful sharing. Similarly, federal policies related to cloud computing and data collected by IoT devices focus on security standards and not on allocating control, access or portability of non-personal data generated by connected products or services.

Currently, the Federal Trade Commission (FTC) and various state Attorneys General (AGs) are taking the

lead in shaping non-personal data handling, using its authority over “unfair or deceptive practices” to police inadequate security and harmful data uses. Enforcement actions increasingly address aggregated datasets, location data, and inferred attributes when their downstream use creates meaningful risk to individuals.

While regulators (at the FTC and the state AGs) may demand reasonable security and truthful representations, they cannot (and do not) impose openended governance frameworks or compel broad data sharing absent clear statutory authority. For in-house counsel, this means enforcement exposure turns heavily on reasonable safeguards, precise disclosures and demonstrable risk management, rather than on compliance with a single, unified data-governance statute.

At present, there is not a clear path to a federal data protection law in the US. In response to the lack of federal legislation, various states have expanded their regulatory regimes to start addressing data sharing and access. Keeping tracking of the various changes in state data protection laws, of which there are currently 19, will be key to managing legal risk.

3.2 Interaction of Data Regulation and Data Protection

In the US, intellectual property rights for non-personal data primarily arise in the context of trade secrets, with access governed by contract, including confidentiality clauses. Data privacy frameworks operate independently and do not overlap with intellectual property rights.

3.3 Rights and Obligations Under Applicable Data Regulation Non-Personal Data

The access to, use of and sharing of non-personal data is primarily governed by contract. Accordingly, parties’ rights and obligations must be determined on a contract-by-contract basis.

Personal Data

The United States lacks comprehensive federal data protection legislation. Instead, personal data is regulated through 19 state privacy laws and various sector-specific federal statutes.

Given this fragmented regulatory landscape, organisations should adopt the following practical approach:

- identify what personal data they collect and process;
- determine which state and federal laws apply to that data; and
- implement a data governance programme that addresses all obligations under the identified laws

Where applicable laws impose overlapping or conflicting requirements, best practice is to adopt the most stringent obligation across all relevant statutes. This “highest common denominator” approach ensures compliance while simplifying operational processes.

3.4 Regulators and Enforcement

The Federal Trade Commission and state AGs serve as the primary enforcers of privacy laws in the United States.

The FTC enforces privacy requirements under Section 5 of the FTC Act, which prohibits unfair or deceptive practices. This authority enables the agency to pursue companies that misrepresent their privacy practices or fail to implement reasonable data security measures.

State AGs enforce privacy requirements under state-specific privacy laws, sector-specific federal laws and state consumer protection statutes.

While there is some co-ordination between the FTC and state AGs, significantly more collaboration occurs among the states themselves. State AGs frequently form coalitions – such as the recent “Consortium of Privacy Regulators” comprising California, Colorado, Connecticut, Delaware, Indiana, New Jersey and Oregon – to conduct multi-state investigations, share technical expertise and address cross-border data issues. This collaborative approach creates a more unified enforcement front and ensures more consistent consumer protection across jurisdictions.

4. Sectoral Topics

4.1 Use of Cookies

The US regulates online tracking technologies – including cookies, pixels, SDKs, mobile advertising IDs, device identifiers, fingerprinting and session replay tools – through a fragmented framework of federal and state laws.

Federal Framework

At the federal level, the regulation of tracking technologies are primarily governed by the following statutes and regulatory bodies.

- FTC Act Section 5 – the Federal Trade Commission prohibits unfair or deceptive practices related to tracking technologies.
- COPPA (Children’s Online Privacy Protection Act) – requires verifiable parental consent (opt-in) before collecting personal information, including persistent identifiers used for tracking, from children under 13 years of age. Enhanced data-retention requirements became effective in June 2025.

State Comprehensive Privacy Laws (State Laws Impose Varying Consent Models)

- California (CCPA/CPRA) – requires businesses to provide opt-out mechanisms for the sale or sharing of personal information, including browsing history and online activity. Enhanced protections apply to minors under 16, requiring affirmative opt-in consent from the consumer (ages 13–15) or parent/guardian (under 13). Businesses must honour Global Privacy Control (GPC) signals as valid opt-out requests.
- Virginia (VCDPA) – requires opt-out mechanisms for targeted advertising and data sales, and mandates opt-in consent for processing sensitive data and data from identified children.
- Colorado (CPA) – defines consent as a “clear, affirmative act” and prohibits dark patterns. Provides detailed technical specifications for universal opt-out mechanisms.
- Connecticut (CTDPA) – permits technology-based opt-out mechanisms and prohibits geofencing for tracking purposes within 1,750 feet of mental health or reproductive health facilities. Opt-in con-

sent is required before the sale of consumer health data.

- Texas (TDPSA) – requires clear, affirmative consent for processing sensitive data and mandates that universal opt-out mechanisms enable consumers to make unambiguous choices to opt out.

Summary of Consent Models

- Opt-in consent required for children under 13 (federal), minors under 16 (California), sensitive data processing (Virginia, Texas) and health data sales (Connecticut)
- Opt-out models apply to targeted advertising and data sales under most state comprehensive privacy statutes, including those in California, Virginia, Colorado, Connecticut and Texas.

Practical Compliance Requirements

Organisations must provide clear, conspicuous notice about tracking practices, implement effective opt-out mechanisms where required, honour universal opt-out signals like GPC in applicable states, ensure consent banners are properly configured and avoid misleading interfaces, establish vendor management processes with contractual protections for third-party tracking providers, and implement data minimisation practices aligned with state law requirements.

Given the complexity of the regulatory landscape, organisations should determine which state and federal laws govern their tracking practices and implement compliance programmes that satisfy the most stringent requirements across all applicable jurisdictions.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised and Targeted Advertising Regulation in the United States

The United States regulates personalised and targeted advertising through a patchwork of federal and state laws. At the federal level, the FTC prohibits deceptive advertising practices and has imposed significant penalties for misrepresenting data collection and use. COPPA essentially bans behavioural advertising to children under 13, requiring verifiable parental consent before collecting any personal information including cookies and device identifiers. HIPAA restricts

healthcare providers from using health information for marketing without authorisation, while GLBA limits financial institutions' ability to share customer data for marketing purposes.

Multiple states – including California, Colorado, Virginia, Connecticut, Utah and Texas – have enacted comprehensive privacy laws governing targeted advertising. These laws generally require businesses to provide opt-out mechanisms for targeted advertising and data sales, often through “Do Not Sell My Personal Information” links on websites. California's law is the strictest, requiring opt-in consent for minors under 16 and mandating recognition of Global Privacy Control signals. All state laws impose heightened protections for sensitive data (health information, precise location, biometric data, race, ethnicity, religion or sexual orientation), requiring affirmative opt-in consent before using such data for advertising. States also prohibit “dark patterns” – manipulative design tricks to obtain consent – and some require risk assessments for profiling activities that could cause unfair treatment or harm.

To comply, companies must:

- post clear privacy notices explaining data collection for advertising;
- provide easy opt-out options for targeted advertising and data sales;
- obtain affirmative opt-in consent for children's data and sensitive information;
- honour universal opt-out signals (like Global Privacy Control) where required;
- avoid manipulative consent interfaces (“dark patterns”); and
- conduct risk assessments for high-risk profiling activities.

Enforcement comes from the FTC and state AGs, with penalties ranging from thousands of dollars per violation to billions for major violations. Given this fragmented landscape, best practice is to identify applicable laws and implement the strictest requirements across all jurisdictions where the business operates.

4.3 Employment Privacy Law

The United States regulates employment privacy through a patchwork of federal and state laws with no single comprehensive federal employment privacy statute. At the federal level, the Electronic Communications Privacy Act (ECPA) generally prohibits intercepting communications but allows businesses to monitor their own systems when clear policies reserve that right. The Stored Communications Act protects against unauthorised access to stored electronic communications. The Computer Fraud and Abuse Act criminalises unauthorised access to computers, creating liability when employers access employee devices without authorisation. The Fair Credit Reporting Act (FCRA) establishes strict requirements for background checks, requiring standalone written disclosure, written authorisation, pre-adverse action notices and certification of compliance with equal employment laws.

State laws vary significantly and often impose stricter requirements than federal law. Wiretapping consent requirements differ by state: California, Illinois and Pennsylvania require all-party consent to record conversations, while many other states operate under one-party consent frameworks. Biometric privacy laws create substantial compliance obligations – Illinois BIPA is the most comprehensive, requiring written notice, disclosure of purpose and retention period and written consent before collecting biometric data like fingerprints or facial scans, with statutory damages of USD1,000–USD5,000 per violation creating significant class action exposure. California's CCPA employment exemptions became inoperative on 1 January 2023, subjecting employee data to notice requirements, access rights, deletion rights and opt-out mechanisms. Virginia, Colorado, Connecticut and Utah generally maintain employment data exemptions from their privacy laws, though this may change.

Workplace monitoring is governed by reasonable expectation of privacy standards, with courts generally finding that clear employer policies reserving monitoring rights eliminate privacy expectations in company-owned systems. However, employees may retain privacy expectations in personal web-based email accounts, attorney-client communications and certain private communications even on company devices. Remote work monitoring raises enhanced

privacy concerns due to home environments where employees have heightened expectations. BYOD (Bring Your Own Device) policies must clearly define employer access rights, specify when device wiping may occur, address data segregation between personal and work information, obtain specific consent for geolocation tracking and implement mobile device management solutions that protect employer data while respecting employee privacy. Processing applicant data requires clear privacy notices, necessary consents (particularly for background checks and biometric screening), FCRA compliance, and in California, CCPA compliance for applicant information.

To comply with employment privacy laws, employers should:

- implement clear monitoring policies notifying employees of surveillance activities and reserving employer monitoring rights;
- obtain appropriate consents for biometric data collection, background checks, and monitoring activities where required by state law;
- provide required notices about data collection, use, and employee rights under applicable privacy laws;
- conduct data protection assessments for high-risk processing activities;
- address multi-state compliance by identifying and applying the most restrictive applicable laws across all jurisdictions;
- manage vendor agreements to ensure third-party service providers meet privacy obligations;
- implement data segregation in BYOD environments to protect both employer and employee interests; and
- maintain detailed records of processing activities, consents and compliance measures

Enforcement comes from the FTC, state AGs, private lawsuits (especially under Illinois BIPA), FCRA class actions and the National Labor Relations Board. Given this complex landscape, employers should assess which laws apply to their operations and implement comprehensive privacy programmes addressing the strictest requirements across all applicable jurisdictions.

4.4 Data Protection in M&A

Given the absence of comprehensive US data privacy requirements, M&A deals require deal-by-deal determinations of applicable data privacy obligations across the transaction lifecycle.

Due Diligence

Buyers should conduct privacy-focused due diligence to assess the target's compliance with applicable state and federal privacy laws, evaluate existing privacy policies and practices, review data processing agreements with third parties, and identify potential liabilities or ongoing investigations.

Representations and Warranties

Asset purchase agreements and equity purchase agreements typically include standard representations and warranties stating that the seller is in compliance with all applicable privacy laws. The onus is on the parties to determine which laws apply to the particular transaction.

Change-of-Control Notifications

Notification requirements for changes of control depend on:

- contractual obligations – many data processing agreements and vendor contracts require notice to customers or data subjects before a change of ownership;
- state privacy laws – some state laws (such as the CCPA) may require updated privacy notices if data practices will materially change post-transaction; and
- sector-specific laws – certain regulated industries (such as healthcare under HIPAA) have specific change-of-control notification requirements.

Post-Closing Integration

Post-closing obligations are determined on a deal-by-deal basis, focusing on which privacy laws apply (state or federal) and what actions the buyer must take under those laws, including updating privacy policies, integrating data governance programmes, harmonising consent mechanisms, and ensuring ongoing compliance with all representations and warranties made during the transaction.

5. International Considerations

5.1 Restrictions on International Data Transfers

The United States regulates cross-border data transfers through a fragmented framework of federal sectoral laws, export controls, national security restrictions and state privacy laws rather than a single comprehensive statute. A “transfer” is defined broadly to include physical movement of data across borders, remote access from abroad, hosting data on foreign servers, disclosure to foreign affiliates or vendors, and granting administrative access to foreign personnel – meaning even allowing an overseas employee to access a US-based database constitutes a transfer. The regulatory landscape encompasses sector-specific federal laws like HIPAA (healthcare data) and GLBA (financial data), which require the same contractual safeguards for international service providers as for domestic ones. Export controls under ITAR prohibit transferring defence-related technical data abroad or to foreign persons within the US without licences. National security frameworks include CFIUS oversight of foreign investments involving sensitive US data and the DOJ Bulk Data Rule effective April 2025, which prohibits data brokers from transferring bulk sensitive personal data to countries of concern (China, Russia, Iran, North Korea, Cuba and Venezuela). State privacy laws in California, Virginia, Colorado, Connecticut, Utah and Texas impose contractual requirements on international processors regardless of data location.

For lawful cross-border transfers, organisations must implement multiple compliance mechanisms depending on applicable laws. Under HIPAA, covered entities must enter into Business Associate Agreements with international third parties handling protected health information, requiring contractual safeguards and application of the “minimum necessary” standard limiting cross-border access. GLBA requires financial institutions to provide privacy notices and opt-out rights before disclosing non-public personal information internationally. State comprehensive privacy laws require written agreements with international processors containing confidentiality obligations, purpose limitations, restrictions on onward transfers without authorisation and compliance assistance requirements. Organisations must conduct risk assessments

evaluating security risks, foreign government access risks and potential data subject impacts before transferring, plus perform vendor due diligence assessing international service provider security controls and compliance capabilities. Contractual agreements must include flow-down provisions ensuring sub-processors receive identical protections. Exceptions exist for consent from individuals (though requirements vary by jurisdiction), necessity for legal proceedings or defending legal rights, law enforcement and national security purposes, and specific business carve-outs in the DOJ Bulk Data Rule.

Cross-Border Transfer Compliance Checklist

- Identify applicable frameworks – determine which federal sectoral laws (HIPAA, GLBA), export controls (ITAR), national security restrictions (CFIUS, DOJ Bulk Data Rule) and state privacy laws apply to transfers.
- Define the transfer – document whether data is being physically moved internationally, allowing remote access from abroad, using foreign hosting, or granting access to foreign personnel.
- Conduct risk assessments – evaluate security risks, foreign government access risks and data subject impacts before making cross-border transfers.
- Perform vendor due diligence – assess international service provider security controls, establish audit rights and verify compliance capabilities.
- Implement contractual safeguards – execute written agreements with foreign processors containing confidentiality provisions, purpose limitations, onward transfer restrictions and security requirements.
- Establish onward transfer controls – include flow-down provisions requiring foreign sub-processors to maintain equivalent protections and notification before engaging new international sub-processors.
- Document legal basis – identify applicable exceptions (consent, legal necessity, law enforcement or business carve-outs) and maintain supporting records.
- Maintain compliance records – keep documentation of risk assessments, international contracts, consent mechanisms and transfer authorisations for regulatory inquiries.

5.2 Government Notifications and Approvals

The United States generally does not require governmental registrations, filings or approvals for routine cross-border transfers of personal data or commercial business data. Federal law imposes no overarching data-export authorisation regime, and state privacy laws (such as the CPRA and VCDPA) require only contractual safeguards – not government permission. Likewise, sector-specific privacy laws (HIPAA, GLBA, FERPA) may restrict disclosure but do not impose approval requirements for international transfers. As a result, typical business and personal-data transfers from the US may proceed without filing.

However, three regulatory regimes – EAR, ITAR, and OFAC – do require licences for exports of certain technology, technical data and software. The Export Administration Regulations (EAR) regulate controlled software and technology and cover electronic, cloud-based and deemed exports, with licensing dependent on ECCN classification, country destination, end-user and end-use. The International Traffic in Arms Regulations (ITAR) require prior authorisation for all exports of defence articles and technical data on the US Munitions List, including deemed exports, and mandate registration with DDTC. The OFAC sanctions regime restricts transfers to sanctioned countries, entities and individuals, with licences required unless a general licence applies. Before any cross-border transfer of data or technology, organisations should classify the item, screen the destination and recipient, assess end-use and determine whether a licence or exception applies; non-controlled business or personal data may be transferred without government involvement.

5.3 Data Localisation Requirements

Data Localisation

The United States has no general requirement that data be stored domestically. Most companies may store data abroad or use foreign cloud providers without seeking government approval. Exceptions primarily arise in government and defence contexts: federal contractors subject to FedRAMP or DFARS/CMMC often must store data on US servers and limit access to US persons, and ITAR-controlled defence technical data cannot be stored overseas or accessed by

foreign nationals without State Department authorisation.

Regulated industries such as banking, healthcare and education may use offshore storage but must maintain strong contractual protections to ensure privacy, security and regulatory access. A 2024 executive order is expected to impose new restrictions on transferring sensitive personal data (such as geolocation, biometrics, genetic data and certain health or financial information) to specific countries of concern, but final rules are still pending. CFIUS may also require US-based storage when foreign investors acquire US companies holding sensitive data. In practice, most commercial data may be stored globally, while government, defence and some categories of sensitive personal information face stricter controls.

Remote Access

For ordinary business and personal data, remote access from outside the United States is generally allowed without government filings. The requirements mirror offshore storage – appropriate contracts, encryption and access controls – but no licensing. However, remote access to controlled technology, such as encryption source code or defence-related technical data, is treated as an export and may require authorisation from BIS (under the EAR) or DDTC (under ITAR) unless an exception applies. Organisations must determine whether the data is controlled, the nationality of the person accessing it, and whether they or their country appear on restricted party lists.

Remote access by persons located in or connected to sanctioned countries such as Cuba, Iran, North Korea, Syria or certain sectors in Russia requires OFAC approval. For federal and defence contractors, remote access from outside the US or by non-US persons is typically prohibited unless explicitly permitted under the contract. Overall, remote access is freely allowed for routine business data but restricted or subject to licensing when involving controlled technology, sanctioned individuals or countries, or federal and defence information.

5.4 Blocking Statutes

No US Blocking Statutes; Courts Retain Discovery Power Despite Foreign Laws

The United States does not have blocking statutes like those found in Europe that categorically prohibit compliance with foreign discovery orders or restrict cross-border disclosures. Unlike many countries that have enacted laws to prevent their citizens and companies from responding to foreign court requests, US law generally facilitates rather than restricts international information sharing and foreign judgment enforcement. States have adopted laws (Uniform Foreign-Country Money Judgments Recognition Acts) that make it easier to recognise and enforce foreign court judgments in the US, not harder. These laws create a presumption in favour of honouring foreign judgments and place the burden on anyone resisting enforcement to prove specific problems with the foreign court's decision.

However, US federal law does create some targeted restrictions. The most significant are Treasury Department sanctions administered by the Office of Foreign Assets Control (OFAC), which prohibit transactions with specially designated nationals and blocked persons from countries like Iran, North Korea, Russia and others. These sanctions can restrict sharing information with sanctioned entities or individuals. Additionally, export control laws (including the International Traffic in Arms Regulations for defence items and Export Administration Regulations for dual-use technology) restrict disclosure of technical data, source code and defence-related information to foreign nationals or entities without proper authorisation. Courts handle these restrictions by issuing specialised protective orders that limit who can access sensitive materials and require compliance with federal export rules.

How US Courts Handle Foreign Blocking Statutes and Privacy Laws

When foreign blocking statutes or privacy laws (like the EU's General Data Protection Regulation) conflict with US court discovery orders, American courts do not simply defer to foreign law. The Supreme Court established in the 1987 *Aerospatiale* case that foreign blocking statutes do not deprive US courts of power to order parties under their jurisdiction to produce evidence, even if doing so violates foreign law. Instead,

courts perform a balancing test (called “comity analysis”) weighing factors like the importance of the evidence to the case, how specific the request is, where the information is located, whether there are alternative ways to get it and the strength of the foreign country’s interest in blocking disclosure.

The modern judicial trend holds that foreign blocking statutes and privacy laws cannot be used to circumvent US discovery rules. Courts have consistently found that the mere existence of foreign laws restricting data disclosure does not prevent American judges from ordering discovery, though these laws may influence whether sanctions are imposed if someone disobeys the order. For example, courts have ruled that even strict privacy laws like the GDPR, which carry significant penalties for violations, cannot be used as an automatic excuse to refuse discovery in US litigation. However, courts recognise genuine conflicts and often use procedural tools to manage them: protective orders limiting who can see sensitive information, requiring the requesting party to pay compliance costs (including costs of meeting foreign privacy law requirements) and demanding indemnification against foreign penalties. Courts also require parties claiming foreign law prevents compliance to provide detailed proof of the specific legal restrictions and show they made good faith efforts to obtain waivers or clarification under foreign law. The bottom line: US courts maintain their authority to order discovery even when foreign laws say otherwise, but they consider foreign legal restrictions when deciding how to structure discovery and whether to penalise non-compliance.

5.5 Recent Developments

The Shift Toward National Security-Driven Restrictions

The United States is moving away from its traditional hands-off approach to data transfers and implementing significant new restrictions based on national security concerns, particularly targeting data flows to China, Russia, Iran, North Korea, Cuba and Venezuela. The most important change is Executive Order 14117 (issued 28 February 2024), which directs the Justice Department to restrict or prohibit American companies from sharing sensitive personal data in bulk – including precise location tracking, biometric data (fingerprints, face scans), genetic information, health records and financial data – with businesses or individuals connected to adversary nations. The Justice Department released a draft framework in April 2024 and is expected to issue proposed regulations in early 2025 with final rules by mid-2025. Once in effect, companies using foreign vendors, cloud providers or employees from these countries who can access large amounts of sensitive US customer data will likely need to implement security programmes (encryption, access controls, auditing) or obtain government approval for certain transactions – the first time the US will require permission or registration for routine data transfers. This represents a fundamental shift: data is now viewed as a strategic national security asset that must be protected from foreign adversaries, not just a consumer privacy issue. Congress has reinforced this approach by passing the TikTok divestiture law (April 2024), which requires ByteDance to sell TikTok or face a US ban because of concerns that the Chinese government could access Americans’ data. The federal government also banned TikTok from all federal devices in late 2022, and over 38 states have done the same. The clear trend is toward more government oversight and restrictions on data flows to geopolitical rivals, driven by concerns about espionage, tracking of Americans and threats to national security.

Trends and Developments

Contributed by:

Paul Lanois
Fieldfisher

Fieldfisher is a European law firm with market-leading practices in many of the world's most dynamic sectors. The firm is a forward-thinking organisation with a particular focus on technology, financial services, energy and natural resources, and life sciences. Fieldfisher chooses a collaborative approach with an intense focus on the end-user and carefully considers how to shape its services to add the most

value to its clients. Many of Fieldfisher's lawyers are widely respected thought leaders, digging deep into the issues that matter most to their clients and providing answers and opinions, not just legalese. The firm's growing European network of offices supports an international client base alongside strategic bases in Silicon Valley and China.

Author



Paul Lanois is a European technology and privacy professional at Fieldfisher based in the Silicon Valley (California) and is an attorney admitted to the Bar in California, New York, the District of Columbia (DC) and the Supreme

Court of the United States. He provides guidance on information governance, data protection, privacy, cybersecurity and digitalisation. In particular, he advises businesses on a wide range of privacy compliance matters, including issues related to privacy and data optimisation, social media integrations, mobile apps, the internet of things and connected devices, and e-commerce and electronic payments. Paul also advises on cybersecurity matters, including on data breaches, incident response, risk assessments, policy development and compliance.

Fieldfisher

2650 Birch Street
Suite 100
Palo Alto, CA 94306
USA

Tel: +1 650 313 2358
Email: info@fieldfisher.com
Web: www.fieldfisher.com

fieldfisher

There was much activity in the data privacy and cybersecurity law space in 2025, as lawmakers, regulators and courts responded to rising cyber threats, rapid technological adoption and growing public concern about data misuse.

The result is a regulatory environment that has become increasingly fragmented, largely because the United States does not have a comprehensive federal privacy law, prompting states to fill this perceived gap with their own state privacy laws, creating a patchwork of overlapping (and sometimes conflicting) obligations for organisations operating nationwide. This state-driven expansion not only broadened the scope of consumer rights and business responsibilities but also introduced compliance challenges for companies navigating divergent requirements across jurisdictions.

At the same time, enforcement activity intensified across federal and state agencies, which shifted from guidance-driven approaches to more aggressive investigations, penalties and enforcement actions. 2025 was also marked by the growing influence of artificial intelligence, which reshaped both the risks regulators were trying to address and the legal frameworks being developed to govern automated decision-making, biometric data and AI-enabled cyberattacks.

Together, these trends and developments made 2025 a year defined by heightened scrutiny, expanding obligations and a more complex compliance landscape than ever before. The below is not intended to be an exhaustive list of all major developments in the US, but rather a list of selected highlights of some developments of significance.

DOJ Finalises Rule on Sensitive Cross-Border Data Transfers

On 8 January 2025, the US Department of Justice issued its final rule implementing Executive Order 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (the "DOJ Rule"). The DOJ Rule took effect on 8 April 2025, and establishes sweeping restrictions on cross-border transfers of bulk US sensitive personal data and US

government-related data to a designated "country of concern", including China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela, as well as to "covered persons" (which are entities or individuals with certain ties to a country of concern). The DOJ Rule also imposes obligations on certain transactions with any foreign person, not only those linked to a country of concern.

The DOJ Rule prohibits US persons from engaging in any "data brokerage" transaction involving specified categories of sensitive US personal data with a country of concern or a covered person. In effect, US data brokers may not license, sell or otherwise transfer a broad range of sensitive US personal data to these entities. The DOJ Rule also bars US persons from engaging in data brokerage transactions involving sensitive US personal data with any foreign person unless the US person imposes contractual safeguards designed to prevent downstream transfers to countries of concern or covered persons. Separately, the DOJ Rule prohibits US persons from knowingly engaging in any "covered data transaction" with a country of concern or covered person that would provide access to bulk human genomic, epigenomic, proteomic, transcriptomic data or to human biospecimens from which such data could be derived.

The DOJ Rule creates a category of "restricted transactions", which include certain vendor, employment and investment agreements that provide countries of concern or covered persons with access to bulk US sensitive personal data or US government-related data. US persons may engage in these transactions, but only if they comply with cybersecurity standards issued by the Cybersecurity and Infrastructure Security Agency (CISA) and meet additional obligations, such as implementing a data compliance programme, undergoing audits and maintaining detailed records.

The DOJ Rule defines sensitive personal data broadly and sets relatively low volume thresholds, meaning that routine online or commercial data collection activities may fall within scope. Many organisations will need to build or significantly expand compliance programmes to meet diligence, auditing, recordkeeping and reporting requirements. Companies should also

review cross-border data flows and update contracts to incorporate the Rule's mandatory safeguards.

Penalties for violations can be significant: civil fines may reach USD368,136 or twice the value of the transaction and wilful violations may result in criminal penalties of up to USD1 million or imprisonment for up to 20 years. The DOJ Rule reflects the DOJ's increasing focus on national security risks associated with data transfers and signals the likelihood of further national security-driven data regulations.

A Slowdown in State Privacy Laws

Despite the introduction of hundreds of consumer privacy bills, 2025 was the first year since 2020 in which no new comprehensive state privacy law was enacted. This leaves the total number of states with comprehensive privacy laws at 19. This does not mean that there was no movement on the legislative side: nine states passed amendments to their existing comprehensive privacy laws in 2025. Those states are Connecticut, Montana, Oregon, Colorado, Kentucky, Texas, Utah, Virginia and California.

State regulators are also stepping up and increasing their collaboration on the implementation and enforcement of their privacy laws with the shared goal of protecting consumers' privacy rights across jurisdictions and ensuring like-minded applications of the applicable laws across jurisdictions. The Consortium of Privacy Regulators was formed as a bipartisan effort that includes the California Privacy Protection Agency and state Attorneys General from California, Colorado, Connecticut, Delaware, Indiana, New Jersey and Oregon.

A Renewed State Focus on AI Legislation

On 23 January 2025, President Trump signed the Executive Order "Removing Barriers to American Leadership in Artificial Intelligence", repealing the previous administration's order on safe and trustworthy AI, and taking aim at the risk of having a patchwork of different state regulatory regimes that could thwart innovation. Nevertheless, in the absence of a broad federal AI regulatory framework, certain US states are passing their own rules, resulting in a mix of federal actions and state laws that companies must follow when building or deploying AI.

Some states have nevertheless introduced state laws governing the use of AI. For example, the Texas Responsible Artificial Intelligence Governance Act (TRAIGA) establishes new obligations for organisations that develop or deploy artificial intelligence systems in Texas, including private entities and government bodies. TRAIGA prohibits the development or deployment of AI systems for certain high-risk purposes, such as intentional unlawful discrimination or other statutorily defined harms, including the creation or dissemination of illegal or explicit content. TRAIGA places limitations on the deployment and development of certain AI systems and went into effect on 1 January 2026, which is one month before the Colorado AI Act.

On 19 December 2025, the New York Governor signed the Responsible AI Safety and Education Act (the "RAISE Act") into law, amending the version that was originally passed by the state legislature in June. The bill creates requirements for the training and use of AI frontier models, including creating a safety plan.

Additionally, California finalised its regulations on cybersecurity audits, risk assessments and automated decision-making technology (ADMT). The regulations went into effect on 1 January 2026, however companies still have some additional time to comply with the new requirements.

Children's Privacy Remains a Concern

In April 2025, the Federal Trade Commission (FTC) issued its final updates to the Children's Online Privacy Protection Act (COPPA) rules, which became effective on 23 June 2025. These amendments broaden the obligations for operators of websites and online services that collect personal information from children under 13. Among the new requirements are the creation of a written children's personal information security programme and enhanced parental controls over how a child's data is used and shared. The amendments also obligate organisations to review and update their data collection, retention, security and disclosure practices to ensure ongoing compliance.

Privacy Enforcement Actions

California remained one of the most active US privacy enforcers in 2025, and two recent actions underscore why global organisations should pay close attention.

In July 2025, the California Attorney General announced what was, at the time, the largest CCPA enforcement action to date: a USD1.55 million settlement with website publisher Healthline, resolving allegations that its use of online tracking technology on its health information website violated the California Consumer Privacy Act (CCPA). According to the Attorney General, an investigation by the California Department of Justice found that the company failed to allow consumers to opt out of targeted advertising and shared data with third parties without CCPA-mandated privacy protections, including data suggesting that a person may have a serious health condition. The settlement also prohibits the company from sharing article titles that reveal that a consumer may have already been diagnosed with a medical condition, effectively banning the company from engaging in these types of data transmissions.

As of the date of this article, the largest CCPA enforcement action was announced in February 2026 against the Walt Disney Company, whereby the company was required to pay USD2.75 million and implement opt-out methods that fully stop the company's sale or sharing of consumers' personal information and fully giving effect to requests for opt-out of the sale or sharing of data across all devices and streaming services associated with such consumers' accounts.

In March 2025, the California Privacy Protection Agency (CPPA) announced its decision against American Honda Motor Co., imposing a USD632,500 penalty for failing to honour opt-out preference signals and for allegedly creating unnecessary friction in the consumer request process. As part of the settlement, the company was required to certify its compliance, train its employees, and consult a user experience (UX) designer to evaluate its methods for submitting privacy requests. The company was also required to change its contracting process to ensure appropriate mechanisms are in place to protect personal information.

In September 2025, the CPPA announced its decision requiring Tractor Supply Company, the nation's largest rural lifestyle retailer, to change its business practices and pay a USD1.35 million fine after the CPPA determined that its privacy notices were insufficient and its opt-out mechanisms ineffective. Notably, this is the first enforcement action involving employment-related data, which is protected under the CCPA (unlike most other state privacy laws), highlighting the importance of privacy notices and privacy rights of job applicants under the CPPA.

California is not the only state that has been active in enforcing privacy laws. In fact, Texas secured a USD1.4 billion settlement (which is one of the largest data privacy-related settlements reached by a single US state) in connection with alleged violations of the Texas Deceptive Trade Practices Act (DTPA) and the Texas' Capture or Use of Biometric Identifier (CUBI) Act. But Texas did not stop there.

In December 2024, the Texas Attorney General (which, in a [press release](#), described Texas as leading the nation in privacy enforcement) brought suits against 14 organisations for alleged violations of the Texas Data Privacy and Security Act (TDPSA) and the Texas Securing Children Online Through Parental Involvement (SCOPE) Act, among other laws. In January 2025, Texas filed the first-ever privacy lawsuit under a state comprehensive privacy law: the lawsuit alleged that a car insurance company developed a software development kit (SDK) which could collect a user's geolocation and movement data. More recently, the Texas Attorney General announced in December 2025 that it has initiated lawsuits against Sony, Samsung, LG, as well as Hisense and TCL for allegedly collecting personal data unlawfully through Automated Content Recognition (ACR) technology included in Smart TVs.

Cybersecurity Remains a Priority for Regulators

In November 2025, amendments to New York Department of Financial Services (NYDFS) Part 500 took effect with enhanced requirements for data security for nearly all covered financial services entities, including multifactor authentication (MFA), asset inventory and data retention.

Contributed by: Paul Lanois, **Fieldfisher**

Conclusion

The US data privacy and cybersecurity landscape continues to evolve in ways that are both expansive and increasingly complex, as we have seen throughout the year 2025. The absence of a comprehensive federal privacy law has further entrenched a fragmented, state-driven regulatory regime, while enforcement authorities have shown a clear willingness to pursue significant penalties and require meaningful operational change. At the same time, national security considerations, children's privacy, and the rapid deployment of AI have emerged as central regulatory priorities, reshaping expectations around data governance, risk management and accountability.

For organisations operating in or targeting the US market, these developments underscore the need for proactive, well-resourced compliance strategies. This includes carefully mapping data flows, reassessing vendor and cross-border transfer arrangements, embedding privacy and cybersecurity by design, and ensuring that internal processes can withstand heightened regulatory scrutiny. Businesses that invest in robust, adaptable compliance programmes will be best positioned not only to manage risk, but also to build trust and resilience in an increasingly demanding regulatory environment.

USA – CALIFORNIA



Trends and Developments

Contributed by:

Christina M. Morgan and David M. Liu
Buchalter LLP

Buchalter LLP is a full-service law firm with over 560 attorneys offering expertise in 35 practice areas. Buchalter's Privacy and Data Security attorneys help clients navigate local, state, federal, and international requirements, including multi-state and multi-national compliance. They advise across industries on website practices, data collection and storage, privacy program development, breach notification obligations, and responding to investigations, penalties, and related litigation. Buchalter's team includes attorneys in major cities across the USA, such as San Diego, Los Angeles, San Francisco, Portland, Seat-

tle, Dallas, and Atlanta. Buchalter's multi-disciplinary team addresses privacy and security issues in litigation, healthcare, intellectual property, finance, corporate, and employment matters. Buchalter delivers timely, strategic, and practical guidance to help clients protect their data and meet evolving regulatory obligations. Buchalter also assists with privacy policies, compliant systems design, due diligence, technology transactions involving personal data, regulatory inquiries, privacy impact assessments, audits, and data subject requests.

Authors



Christina M. Morgan is a Certified Information Privacy Professional (CIPP/US) and co-chair of the Privacy and Data Security practice group at Buchalter LLP. She is well versed in consumer privacy laws, including the

California Consumer Privacy Act (CCPA) and the Texas Data Privacy and Security Act (TDPSA). Ms Morgan routinely conducts privacy reviews and counsels clients on privacy compliance and consent management. She has prepared myriad policies and terms for client websites, including privacy policies, notices of collection, and terms of service. Ms Morgan also supports clients who are sharing personal information with vendors and other third parties by negotiating data processing agreements.



David M. Liu is co-chair of the Cyber Investigations and Data Rights Enforcement and Artificial Intelligence practice groups at Buchalter LLP. David specialises in cybersecurity, privacy litigation, class actions,

mortgage lending and real estate. David's practice focuses on the defence of data breach class actions, mass arbitrations and individual actions involving state and federal privacy laws including CIPA, CCPA/CPRA, and CMIA. David also counsels individuals, companies (including Fortune 500 companies), international transportation providers, banks and financial institutions, in complex commercial litigation and class actions; misappropriation of trade secrets; partnership, investor and shareholder disputes; business torts; contract claims; real property disputes; and federal government forfeiture actions for real property.

Buchalter LLP

655 West Broadway
Suite 1600
San Diego
California 92101
USA

Tel: +1 (619) 219 5335
Fax: +1 (619) 219 5344
Email: cmorgan@buchalter.com
Web: www.buchalter.com

Buchalter

The California Consumer Privacy Act of 2018 Remains One of the Strictest Consumer Privacy Laws in the Nation

The California Consumer Privacy Act of 2018 (CCPA), as amended, gives consumers the following rights:

- the right to limit the use and disclosure of sensitive personal information collected about them;
- the right to opt out of the sale of their personal information and the right to opt out of the sharing of their personal information for cross-context behavioural advertising;
- the right to correct inaccurate personal information that businesses have about them;
- the right to know what personal information businesses have collected about them and how they use and share it;
- the right to equal treatment (ie, non-discrimination); and
- the right to delete personal information, subject to some exceptions.

Businesses must provide methods by which consumers can exercise these rights. The CCPA imposes certain disclosure obligations, including the posting of a notice at collection and a privacy policy.

California Created the First, and Only, Privacy Enforcement Agency in the United States

In 2020, California voters approved the California Privacy Rights Act of 2020, which amended the CCPA. Among other things, the California Privacy Rights Act created a new agency to implement and enforce

the CCPA – the California Privacy Protection Agency (CPPA). The CPPA is responsible for:

- promoting public awareness of consumers' rights and businesses' responsibilities under the CCPA;
- adopting regulations in furtherance of the CCPA;
- enforcing the CCPA through investigations, audits, and enforcement actions;
- co-operating with other agencies with jurisdiction over privacy laws to ensure consistent application of privacy protections; and
- providing technical assistance and advice to the legislature with respect to privacy-related legislation.

With New Regulations Come Increased Compliance Obligations

On 23 September 2025, the CPPA announced the approval of new regulations. Most notably, the new regulations require businesses to complete annual cybersecurity audits and conduct risk assessments before certain processing activities. The new regulations also require that consumers be given the opportunity to opt out of the business's use of automated decision-making technology.

The new regulations, described below, went into effect on 1 January 2026.

Cybersecurity audits

Every business whose processing of consumers' personal information presents a significant risk to consumers' security is required to complete an annual

cybersecurity audit. Processing of personal information presents significant risk to consumers' security if:

- the business derived 50% or more of its annual revenue from selling or sharing consumers' personal information in the preceding calendar year; or
- the business had annual gross revenue in excess of USD25 million in the preceding calendar year and:
 - (a) processed personal information of 250,000 or more consumers or households in the preceding calendar year; or
 - (b) processed the sensitive information of 50,000 or more consumers in the preceding calendar year.

Businesses must use a qualified, objective, independent professional using procedures and standards recognised within the auditing profession. Businesses must make good-faith efforts to disclose all relevant facts and make sure the auditor has access to all relevant information. Attestations are insufficient.

The audit must assess how the business's cybersecurity programme protects personal information from unauthorised access, destruction, use, modification, or disclosure, and protects against unauthorised activity resulting in the loss of availability of personal information. This includes evaluating the strength of passwords, the use of multi-factor authentication, encryption practices, account management and access controls, the security of hardware and software being used by the business, and network defences.

Once an audit report is complete, the business must certify to the CPPA that it has completed the required audit. The certification must be completed by a member of the business's executive management team.

When a business must start completing cybersecurity audits depends on the business's annual revenue.

Businesses with more than USD100 million in annual gross revenue in 2026 must comply with the new audit requirements by 1 April 2028. The audit should cover 1 January 2027 through 1 January 2028.

Businesses with annual gross revenue between USD50 million and USD100 million in 2027 must comply with the new audit requirements by 1 April 2029. The audit should cover 1 January 2028 through 1 January 2029.

Businesses with less than USD50 million in annual gross revenue in 2028 must comply with the new audit requirements by 1 April 2030. The audit should cover 1 January 2029 through 1 January 2030.

After 1 April 2030, businesses must complete an audit that covers the calendar year. The audit report must be completed by 1 April of the following year.

Risk assessments

Every business whose processing of consumers' personal information presents significant risk to consumers' privacy must conduct a risk assessment before initiating that processing. The following processing activities present a significant risk to consumers' privacy:

- selling or sharing personal information;
- processing sensitive personal information;
- using ADMT for a significant decision concerning a consumer;
- using automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behaviour, location, or movements, based on:
 - (a) a systematic observation of that consumer when they are acting in their capacity as an educational programme applicant, job applicant, student, employee, or independent contractor for a business, or
 - (b) the consumer's presence in a "sensitive location", such as a hospital, pharmacy, domestic violence shelter, or food pantry;
- processing personal information that the business intends to use to train:
 - (a) an ADMT for a significant decision concerning a consumer;
 - (b) facial recognition technology;
 - (c) emotion recognition technology; or

- (d) other technology that verifies a consumer's identity or conducts physical or biological identification or profiling of a consumer.

The purpose of a risk assessment is to determine whether the risks to consumers' privacy from the processing outweigh the benefits to consumers, the business, other stakeholders, and the public. The goal is to restrict or prohibit the processing of personal information if the risks to privacy outweigh the benefits of processing.

Risk assessments must be revisited at least once every three years, or whenever there is a material change relating to the processing activity, to ensure they remain accurate. Businesses must retain their risk assessment for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.

As with cybersecurity audits, certain information about risk assessments must be reported to the CPPA. For risk assessments conducted in 2026 and 2027, the business must submit the required information no later than 1 April 2028. For risk assessments conducted after 2027, the business must submit the required information no later than 1 April of the following year.

Automated decision-making technology

The new regulations impose additional obligations on businesses that use "automated decision-making technology", or ADMT, to make a significant decision concerning a consumer. ADMT is defined as any technology that processes personal information and uses computation to replace human decision-making or substantially replace human decision-making. A significant decision is one that results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services.

A business that uses ADMT to make a significant decision must provide consumers with a prominent and conspicuous pre-use notice. Among other things, the pre-use notice must include a link through which consumers can opt out of the business's use of ADMT. There must be two or more methods to opt out of

ADMT. When developing these methods, the business must consider how the consumer ordinarily interacts with the business. The method of opting out must be easy and require minimal steps.

In addition, a business must provide consumers with the following information upon request:

- the specific purpose for which the business used ADMT;
- information about the logic of the ADMT;
- outcome of the decision-making process for the consumer, including how the business used the output of the ADMT to make a significant decision with respect to the consumer; and
- notice that the business is prohibited from retaliating against consumers who make such requests.

Businesses must comply with these ADMT provisions by 1 January 2027.

California Has Increased Its Enforcement Activity

Since its creation in 2020, enforcement actions have steadily increased in both number and severity. For example, on 30 September 2025, the CPPA announced a record USD1.35 million fine against Tractor Supply. The CPPA alleged that Tractor Supply:

- failed to maintain an adequate privacy policy notifying consumers of their rights;
- failed to provide adequate privacy notices to consumers and job applicants;
- did not implement effective opt-out mechanisms, including browser-based Global Privacy Control signals; and
- lacked CCPA-compliant data sharing agreements with other companies.

In addition to the penalty, Tractor Supply was ordered to conduct quarterly scanning of digital properties, update its processes for handling opt-out requests, amend its third-party contracts, and have a senior officer or director certify its compliance with the CCPA annually for the next four years.

Soon after, on 11 February 2026, the California Attorney General announced a settlement of USD2.75 million with Disney. The Attorney General alleged that

Disney did not have effective opt-out mechanisms. The opt-out toggle only applied the request to the specific streaming service the user was watching and often only the specific device being used. Webform opt-outs were not effective for embedded third-party tracking pixels. Global Privacy Control signals were only honored on the device used to make an opt-out request rather than on all user devices. Based on Disney and other recent settlements, user opt-outs appear to be a high priority for the Attorney General.

The CPPA Also Implements and Enforces Laws Relating to Data Brokers

A “data broker” is a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Data brokers must register with the CPPA on or before 31 January of each year.

Data brokers must register for California’s accessible deletion mechanism, referred to as “DROP” (Delete Requests and Opt-Out Platform). Data brokers must check the platform at least once every 45 days then: (i) process all requests, and (ii) direct all service providers or contractors to delete the consumer’s personal information, as well.

In addition, data brokers must make additional disclosures in their privacy policy. Namely, by 1 July 2026, data brokers must disclose:

- the number of deletion requests received in the previous calendar year;
- the number of requests complied with in the previous calendar year;
- the number of requests denied in the previous calendar year, along with the reason(s) for the denial; and
- the median and mean number of days that it took to respond to requested received during the previous calendar year.

Further, starting on 1 January 2028, and every three years thereafter, data brokers must undergo an audit by an independent third party to determine compliance with the data broker statutes.

Businesses Operating in California Are Also Facing a Wave of Litigation Relating to the Use of Third-Party Cookies and Tracking Technologies

The California Invasion of Privacy Act (CIPA) is a criminal statute enacted in 1967. In addition to criminal liability, it creates a private right of action for acts such as wiretapping, eavesdropping, and the use of a pen register. Enterprising attorneys have taken this law and applied it to new, web-based technologies, such as third-party cookies.

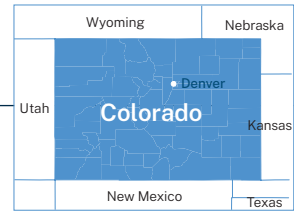
There are two primary theories. One, that the use of third-party cookies constitutes wiretapping, because the cookies read or attempt to read the contents of a communication between the website and its visitor without the visitor’s consent. Two, the cookies or tracking technologies are “pen registers” because they are devices or processes that record electronic communications.

There is not uniform treatment of these claims by the courts. However, we are seeing more and more federal courts allow these claims to proceed, while state courts tend to be more skeptical.

CIPA imposes a fine of USD2,500 per violation. Typically, these suits are brought by individual plaintiffs and seek damages of approximately USD30,000. However, there is a risk of a class action, which could expose businesses to significant liability.

There have been several attempts by the legislature to limit these claims. Most recently, on 3 June 2025, the California Senate passed Senate Bill 690, which would create a “commercial business purpose” exception to CIPA. The bill is still active; it is in the committee process. Until this or a similar law is passed, many businesses are implementing new cookie practices, akin to the European standard, to reduce their risk of CIPA liability.

USA – COLORADO



Trends and Developments

Contributed by:

Daniel Pietragallo and Douglas DePeppe
Buchalter LLP

Buchalter LLP is a full-service law firm with over 560 attorneys offering expertise in 35 practice areas. Buchalter's Privacy and Data Security attorneys help clients navigate local, state, federal, and international requirements, including multi-state and multi-national compliance. The firm advises across industries on website practices, data collection and storage, privacy programme development, breach notification obligations, and responding to investigations, penalties, and related litigation. The team includes attorneys

from multiple practice areas who address privacy and security issues in litigation, healthcare, intellectual property, finance, corporate, and employment matters. The firm delivers timely, strategic, and practical guidance to help clients protect their data and meet evolving regulatory obligations. Buchalter also assists with privacy policies, compliant systems design, due diligence, technology transactions involving personal data, regulatory inquiries, privacy impact assessments, audits, and data subject requests.

Authors



Daniel Pietragallo is special counsel in the Denver office of Buchalter LLP, a member of the Intellectual Property group, and co-chair of the Artificial Intelligence industry group. A former Senior Assistant Attorney General for

Colorado and former Assistant District Attorney in Allegheny County, he focuses on white-collar litigation, cybersecurity, data privacy, and AI governance. He teaches Cybersecurity, Data Privacy, and Incident Response as an Adjunct Professor at the University of Denver. He holds IAPP certifications including AIGP, CIPP/US, and FIP, and serves on the Rocky Mountain Cyber Fraud Task Force and various AI governance working groups, including the Sedona Conference.



Douglas DePeppe is special counsel in the Denver office of Buchalter LLP, focusing nationally on data rights, data protection, sports data licensing, and cybersecurity law. A retired Army Judge Advocate, he helped develop

cybersecurity law capabilities for the Army JAG Corps and later at Homeland Security, including serving as legal adviser to US-CERT. His work includes breach response and crisis management as a Breach Coach, and he has spent twenty years assisting clients with cyber-attacks. Widely respected in the field, he has presented globally and published in Forbes, trade journals, and other outlets.

Buchalter LLP

1099 18th Street
Suite 1900
Denver
CO 80202-1905
USA

Tel: +1 (303) 253 6740
Email: dpietragallo@buchalter.com
Web: www.buchalter.com

Buchalter

Colorado is consistently at the forefront of technology and data governance regulation at the state level and is poised to maintain that position in 2026. Current legal trends include amendments to the Colorado Privacy Act regarding biometric data, online privacy for children, and the ongoing debate surrounding the implementation of SB24-205 (the Colorado AI Act).

The Colorado AI Act was signed into law in 2024 and is the first comprehensive risk-based AI governance regulation in the United States. It seeks to prevent algorithmic discrimination by regulating high-risk AI systems. Although the law is subject to additional debate during the current legislative session, the structural framework will likely remain intact with enforcement starting during 2026.

Updates to the Colorado Privacy Act

The Colorado Privacy Act (CPA) was one of the first comprehensive state-level privacy laws in the United States and became effective on 1 July 2023. The CPA grants Colorado consumers the right to access, correct, delete, and opt out of automated processing of their personal information for targeted advertising, sale, and certain forms of profiling. The CPA applies to controllers processing the personal information of 100,000 or more Colorado consumers annually or deriving revenue from the data of 25,000 or more Colorado consumers.

The CPA imposes heightened obligations on the processing of sensitive data, which it defines to include racial or ethnic origin, religious beliefs, mental or physical health conditions, sexual orientation or gender identity, citizenship, or immigration status, genetic or biometric data, personal data from known children, and precise geolocation data. Controllers may not process sensitive data without first obtaining the consumer's consent.

Controllers must also conduct and document data protection assessments for processing activities that present heightened risk, including the processing of sensitive data, the sale of personal data, and processing for targeted advertising or certain forms of profiling. These data protection assessments must be provided to the Colorado Attorney General upon request and robust documentation serves as the best

defence against a regulatory inquiry. In the wake of a data breach, the absence of a well-documented assessment can be a significant liability, both in regulatory proceedings and in civil litigation.

Building on the foundation established in the Colorado Privacy Act, HB 24-1058 expanded the definition of "sensitive data" in the CPA to include biological data and neural data. The law defines "sensitive data" to include genetic, biometric, or biological data processed for the purpose of identifying any individual, or personal data from a known child.

HB 24-1130 further amended the Colorado Privacy Act to add protection for the collection of biometric data, including establishing a retention schedule and protocols for responding to a data security incident. The law specifically prohibits the collection of biometric identifiers unless the controller obtains consent from the consumer and prohibits the sale, lease, or trade of any biometric data.

Additionally, SB24-041 amends the Colorado Privacy Act to provide specific protection for children's online privacy. The law limits the collection of precise geolocation data and requires online services to obtain consumer consent before processing a minor's personal data for targeted advertising, sale, or profiling.

From a compliance standpoint, the ongoing evolution of the Colorado Privacy Act will present challenges for companies who deal in the collection, processing, and transfer of sensitive data. Colorado continues to aggressively expand the scope of consumer rights in the CPA and create new compliance obligations for business. Any company doing business in one of the above-referenced sectors should consult with privacy experts to better understand their obligations and mitigate potential risk exposure.

The Colorado AI Act (SB 24-205)

On 17 May 2024, Colorado Governor Jared Polis signed into law SB 24-205, which became the first comprehensive risk-based AI governance law in the United States. Although other states have passed AI governance and transparency laws, the Colorado AI Act creates many unique burdens for developers and deployers of high-risk AI systems, including documen-

tation requirements, risk assessments, self-reporting requirements, data subject rights, and impact assessments. The law continues to be the subject of much debate, and the governor has convened a working group of diverse stakeholders to continue negotiating refinements to the law in the current legislative session.

The law “Concerning Consumer Protections in Interactions with Artificial Intelligence Systems” is also known as the “Colorado Anti-Discrimination in AI Law” (ADAI) or the Colorado AI Act. The Colorado Attorney General is charged with rulemaking and enforcement authority and there is no private right of action. The law is currently scheduled to go into effect on 30 June 2026.

While the law focuses on developers and deployers of high-risk AI systems, it also requires disclosure to consumers when they are interacting with any AI system in situations where it would not be obvious. This disclosure obligation applies broadly, not just to high-risk deployers but any company using consumer-facing artificial intelligence systems. The notification requirements also include disclosure to consumers about the right to opt-out of automated decision-making.

Consequential decisions, algorithmic discrimination and high-risk AI systems

The Colorado AI Act defines “algorithmic discrimination” as any circumstance where the use of artificial intelligence creates a condition involving “an unlawful or differential treatment that disfavours an individual or group”. Unlike traditional anti-discrimination laws, the Colorado AI Act is proactive in nature by seeking to prevent algorithmic discrimination before it occurs. The law places the burden on businesses using high-risk AI systems to prove non-discrimination through governance, oversight, and safety testing.

A consequential decision is defined as one that “has a material legal or similarly significant effect on the provision or denial to any consumer, or the cost or terms of” opportunities, goods, or services. The statute further defines eight presumptive categories of consequential decisions, which include:

- employment or an employment opportunity;
- a financial or lending service;
- an essential government service;
- healthcare services;
- housing;
- insurance; and
- a legal service.

Notably, these categories track closely with the high-risk categories listed in Annex III of the European Union’s AI Act, but the risk-based approach is unique among US states.

A high-risk artificial intelligence system is one that either makes a consequential decision or is a substantial factor in making a consequential decision. Consequential decisions made by AI systems will be subject to heightened obligations if they affect a consumer’s education, employment, banking, public benefits or services, healthcare, housing, insurance, or legal rights. Importantly, the law prohibits disparate treatment related to access to goods or services, as well as the cost and terms of those services.

From a compliance standpoint, the broad scope of services where AI systems could affect consequential decisions means the law will apply to many businesses in Colorado, some of which are using AI but lack the policies and procedures to withstand regulatory scrutiny. Colorado’s landmark AI law has broad application for both developers and deployers of high-risk AI systems across a wide range of potential services. Any company doing business in one of the above-referenced sectors should consult with AI governance experts to better understand the obligations and mitigate potential risk exposure.

Developers and deployers

The Colorado AI Act regulates developers and deployers of high-risk AI systems when used as a substantial factor in making a consequential decision. A deployer is anyone doing business in the State of Colorado that uses a high-risk AI system as a substantial factor in making a consequential decision, while a developer is anyone doing business in Colorado that develops or intentionally and substantially modifies an AI system.

- education enrolment or an education opportunity;

Examples of companies that are AI developers include providers like Open AI (ChatGPT), Anthropic (Claude), Microsoft (Copilot), or Google (Gemini). However, smaller companies that would otherwise be considered deployers can become developers if they intentionally modify an AI system. In such instance, the company would assume all the same obligations as larger developers.

Under the law, both developers and deployers of high-risk AI systems have a duty to avoid algorithmic discrimination. Developers are required to provide documentation about the risks, benefits, and intended use of each AI system, as well as high-level summaries of training data, documentation regarding governance, safety testing, and impact assessments.

Deployers of high-risk AI systems are obligated to conduct impact assessments and implement a risk-management programme that incorporates policies and practices to mitigate the risk of algorithmic discrimination. Deployers have a duty to disclose the high-risk AI system to consumers before processing and notify consumers of the right to opt-out. Deployers must also provide an explanation about the nature of automated decision-making and the basis on which the decision was made, including the extent to which the AI contributed to the decision.

Requirements for adverse consequential decisions

Under the Colorado AI Act, adverse consequential decisions trigger additional consumer rights and corporate obligations, which include the following requirements:

- a statement disclosing the principal reason for the consequential decision, including:
 - (a) the degree and manner in which the AI system contributed to the consequential decision; and
 - (b) the type of data processed to make the high-risk decision;
- the source of the data processed to make the high-risk decision;
- the opportunity to correct any inaccurate personal data; and
- the opportunity to appeal an adverse consequential decision with “human review”.

To use one prominent example of a high-risk AI system, most online job portals implement artificial intelligence to scan and sort resumes through an applicant tracking system (ATS). Under the current iteration of the Colorado AI Act, using an ATS to sort resumes would constitute high-risk processing if it is used as a substantial factor in making a consequential decision about an employment opportunity. Because most ATS systems determine which candidates move forward in the selection process and which candidates do not, resume filtering and stack-ranking systems would be considered high-risk. Under this example, each company that uses an AI system to sort resumes would be subject to the high-risk processing requirements of the Colorado AI Act if that system affects Colorado consumers.

Because the law applies broadly to companies using AI affecting Colorado consumers, the online nature of business will require compliance from companies located outside of the Rocky Mountain Region. Companies using AI systems to make consequential decisions should carefully consider the benefits and obligations associated with continued high-risk processing.

Risk management frameworks, impact assessments, and enforcement

The Colorado AI Act requires each deployer of a high-risk AI system to implement a risk management policy and programme to ensure an iterative process of corporate governance. The risk management framework must be appropriate for the size and complexity of the deployer and the nature and scope of the high-risk processing. The law specifically references the National Institute of Standards and Technology (NIST) AI governance framework and International Standards Organization (ISO) 42001 as acceptable AI risk management frameworks and offers an affirmative defence if a company discovers and cures a violation but is otherwise in compliance with one of those frameworks. Businesses looking to mitigate regulatory risk associated with the use of AI systems would be well-served by selecting and implementing one of the approved governance frameworks.

The Colorado Attorney General’s rule-making authority includes establishing requirements for docu-

mentation, risk management programmes, impact assessments, and affirmative defences. The Colorado Attorney General's enforcement authority also provides the right to inspect any company's risk management policy, impact assessment, or records to ensure compliance. This broad oversight authority will allow the Colorado Attorney General to identify those companies that have implemented the required governance structures and those that lack appropriate corporate governance. There is no private right of action associated with this law.

What next for the Colorado AI Act?

In August 2025, following a special legislative session that resulted in little progress, the legislature agreed to delay enforcement of SB 24-205 until 30 June 2026. However, negotiations between consumer and industry groups are ongoing and may yield minor changes to the law before it goes into effect. An additional delay of enforcement until January of 2027 is also a possibility.

Proposed modifications to the law include a focus on Automated Decision-Making Technology (ADMT), which aligns with language in the California Consumer Privacy Act (CCPA). Despite the potential for delayed implementation enforcement and further changes to the law, the era of comprehensive state-level AI governance regulation is upon us with the coming implementation of the Colorado AI Act.

For companies using AI systems to make consequential decisions, waiting until the enforcement date to develop a compliance strategy creates increased regulatory risk. Colorado's law is structurally closer to the EU AI Act than any other US state law and stands out for its heightened risk-based regulatory requirements. Colorado's AI Act will usher in a new era of comprehensive state-level AI governance, regulation and enforcement in 2026.

USA – FLORIDA



Trends and Developments

Contributed by:

Jason Loring, Andrew Lee and Lara Sevenser
Jones Walker LLP

Jones Walker LLP has a privacy, data strategy and artificial intelligence team that helps clients with a full spectrum of data privacy, data protection and AI solutions, including identifying, preventing and responding to data incidents, contracting and transactional support, emerging technology guidance, and litigation and dispute resolution, all while managing and mitigating related risks. Its interdisciplinary team brings together highly experienced attorneys with professional backgrounds in a wide range of industries, including banking and financial services, health-

care, technology, telecommunications, energy, petrochemical, maritime, consulting, government, digital commerce and retail. Staying on top of legal, compliance and regulatory obligations under the myriad of burgeoning global privacy, data protection, and AI-related laws, regulations, frameworks and standards can be challenging for any organisation, large or small. Jones Walker has the knowledge and practical experience to help clients navigate these laws, obligations frameworks and standards. Timely insights can be found at www.AILawBlog.com.

Authors



Jason Loring is a partner in the corporate practice at Jones Walker and co-leads the firm's privacy, data strategy and artificial intelligence team. He advises clients on data privacy and protection, cybersecurity,

data governance, breach response, data strategy, and AI and machine learning, as well as strategic technology transactions and related commercial matters. Jason focuses his practice on data privacy, data protection, cybersecurity, AI adoption, deployment, and risk mitigation, privacy assessments and audits, data innovation, incident response and proactive incident readiness, vendor and outsourcing agreements and contracts, and related legal and regulatory matters.



Andrew Lee founded and serves as co-leader of Jones Walker's privacy, data strategy and artificial intelligence team and holds the CIPP/US designation from the International Association of Privacy Professionals.

Andy also chairs the firm's innovation committee and co-leads the technology industry team. Andy's data privacy and security work involves advising clients in the areas of data privacy and cybersecurity resilience and recovery. He helps develop,

implement and enforce policies and procedures to ensure defensible, repeatable and efficient processes and programmes related to the security of sensitive corporate data, recovery after cyber intrusions, litigation defence and prosecution, and complex electronic discovery of data in legal proceedings and internal investigations.



Lara Sevenser is a partner in the corporate practice group and co-leader of the technology industry team at Jones Walker. Lara's practice focuses on advising clients with respect to strategic commercial

contracting as well as drafting and negotiating complex technology, outsourcing and digital transactions. She has represented international and domestic businesses, including publicly traded corporations, privately held companies, utilities and partnerships in multimillion-dollar transactions domestically and globally. She regularly advises on the use, licensing, acquisition and commercialisation of intellectual property, including matters regarding privacy and data protection. Prior to joining Jones Walker, Lara served as global lead procurement, technology and outsourcing counsel for a leading global audit and consulting organisation.

Jones Walker LLP

Brickell World Plaza
600 Brickell Avenue
Suite 3300
Miami, Florida, 33131
USA

Tel: +1 404 870 7531
Email: jloring@joneswalker.com
Web: www.joneswalker.com



Florida's Privacy Landscape: A Targeted Approach

Unlike broad consumer privacy laws adopted by other states, Florida's framework is intentionally narrow, targeted and politically shaped. Florida focuses on Big Tech monopolies, foreign ownership risks and AI accountability rather than generalised privacy compliance. The result: Many businesses operate without comprehensive privacy obligations, while a select few face intense scrutiny. As 2026 unfolds, Florida's strategy is generating significant enforcement actions and legislative momentum that warrant close attention.

With a selective approach to privacy, many businesses are outside the scope of Florida's omnibus consumer privacy rights law, the Florida Digital Bill of Rights (FDBR) but still face breach notification and security duties under the Florida Information Protection Act (FIPA), and they may have additional obligations if their online platforms or services are directed at, or substantially used by, minors. Florida has no general privacy notice requirement for most companies, no mandated consumer rights mechanisms, and no affirmative data governance obligations outside the narrow FDBR context. Certain categories, however, do face heavy scrutiny: Big Tech platforms subject to the FDBR, foreign-owned healthcare companies collecting biometric or demographic data and operators of AI systems interacting with children. Understanding whether an organisation falls into one of these targeted categories is essential for 2026 compliance planning.

The Florida Digital Bill of Rights: A Big Tech Law

The FDBR took effect in July 2024 and targets the world's largest technology platforms. The law applies exclusively to controllers with more than USD1 billion in global gross annual revenue that also meet one of three criteria: (i) derive 50% or more of revenue from online advertising, (ii) operate a smart speaker or voice command service not integrated into vehicles, or (iii) operate an app store with at least 250,000 applications. This threshold limits coverage to a small group of global platforms such as Google, Meta, Apple and Amazon, while exempting mid-market businesses entirely. (Importantly, Florida imposes no comprehensive privacy programme, notice or data rights obligations on mid-market or small businesses.)

For covered entities, the obligations are substantial. The FDBR provides Florida consumers with access, correction, deletion and portability rights, plus the ability to opt out of targeted advertising, sales and profiling activities. Controllers must respond to consumer requests within 45 days, with a possible one-time extension of 15 days when reasonably necessary. The law requires controllers to provide at least two accessible methods for consumers to submit requests, accommodating how consumers normally interact with the controller.

Controllers must conduct data protection assessments for high-risk processing activities. These assessments must identify and weigh the benefits and risks of processing, considering the use of de-identified data, reasonable consumer expectations and the relationship between controller and consum-

er. Required assessments cover targeted advertising, sale of personal data, profiling that presents reasonably foreseeable risks, processing of sensitive data and other processing involving heightened risk. These assessments must be documented and made available to the Florida Department of Legal Affairs (the “Department”) upon request.

Enforcement rests exclusively with the Department, which can assess penalties of up to USD50,000 per violation, tripled for violations involving children or failures to honour deletion and opt-out requests. The law provides a 45-day cure period for alleged violations, though this opportunity does not apply to violations that knowingly involve children. If, after notification of an alleged violation, the entity cures the violation within 45 days and provides proof to the Department, no enforcement action can proceed, though the Department may issue a letter of guidance that no future cure period will apply.

First Enforcement: The Roku Action

In October 2025, Attorney General (AG) James Uthmeier brought Florida’s first FDBR enforcement action against video streaming provider Roku. The complaint alleged that Roku collected and sold children’s sensitive data without obtaining required consent and notice, enabled reidentification of children’s data and failed to provide effective privacy controls and opt-out mechanisms, violating both the FDBR and the Florida Deceptive and Unfair Trade Practices Act.

This enforcement action signals several enforcement priorities for the AG’s office. First, protection of children’s data receives heightened attention, consistent with the statute’s tripled penalties for violations involving minors. Second, transparency in data sales practices is non-negotiable; controllers must clearly disclose when they sell personal data and provide effective opt-out mechanisms. Third, the AG expects covered entities to obtain affirmative consent before collecting children’s information, not merely rely on age-neutral consent mechanisms.

The timing of the Roku action, coming barely 15 months after the FDBR’s effective date, signals that Big Tech platforms subject to the law should expect active enforcement. Covered entities should review

their practices with regard to collection of children’s data, data sales disclosures and opt-out mechanisms to ensure compliance.

The CHINA Prevention Unit: Targeting Foreign-Owned Healthcare Companies

While FDBR enforcement has begun targeting platform behaviour, Florida’s privacy regulators are also targeting a different category of risk: foreign ownership and sensitive data collection.

In February 2026, Uthmeier announced the creation of the CHINA Prevention Unit, a specialised enforcement initiative within the AG’s office investigating foreign corporations, particularly those with Chinese ownership, that collect consumer data from Florida residents. The AG’s office has identified healthcare as a primary enforcement focus, citing concerns that sensitive health data may be shared with foreign adversaries. The unit has already issued subpoenas to medical device manufacturers, including demands for audits to identify ties to China and verify whether biometric or patient data is being transmitted to foreign servers.

This development creates immediate compliance risks for healthcare technology companies with foreign ownership or investment. The CHINA Prevention Unit’s mandate encompasses Florida’s data breach notification law, data security requirements and consumer protection statutes. Its creation reflects concerns that foreign adversaries could exploit health data access for intelligence purposes, individual targeting or infrastructure vulnerability assessment.

Telehealth platforms, health and fitness apps, genetic testing companies and medical device manufacturers with foreign ties should conduct ownership structure assessments and data transfer audits. Key compliance steps include documenting the corporate ownership chain, mapping data flows to determine whether personal information is transferred internationally and assessing whether business relationships with foreign entities create exposure under the CHINA Prevention Unit’s mandate.

The CHINA Prevention Unit reflects broader concerns about foreign access to sensitive health information.

As healthcare increasingly relies on technology platforms, the collection of biometric identifiers, genetic data and detailed health metrics through wearable devices, mental health apps and genetic testing services has grown dramatically. Florida's enforcement strategy suggests these practices will face heightened scrutiny when foreign entities are involved, either through direct ownership or through data sharing arrangements.

Artificial Intelligence Regulation: From Transparency to Rights

Florida is pursuing comprehensive AI regulation through initiatives addressing government use, consumer protection and children's safety.

The Florida Artificial Intelligence Bill of Rights (SB 482), currently advancing in the 2026 legislative session (building on Gov. Ron DeSantis' 2025 AI safeguards initiative), would establish significant consumer-facing AI rules, particularly for companion chatbots and data handling. The bill would require AI companies to provide parental controls allowing parents to access conversations their children have with companion chatbot platforms and large language models. This provision addresses growing concerns about children developing relationships with AI systems, receiving advice on sensitive topics without parental knowledge, or being exposed to inappropriate content through conversational AI interfaces.

The parental access requirement would create significant technical and operational challenges. Companies would need to implement age verification systems, develop secure portals for parental access and establish clear data retention policies.

The legislation would also restrict the sale or sharing of personal identifying information with third parties unless properly de-identified and would limit state agencies from using AI providers with certain foreign affiliations, reflecting national security and data sovereignty concerns similar to those underlying the CHINA Prevention Unit's creation.

If enacted, SB 482 would position Florida alongside Colorado and California as a leader in AI regulation. Colorado's AI Act focuses on algorithmic discrimina-

tion in consequential decisions. California's various AI initiatives address deepfakes, automated decision-making and AI safety. Florida's approach emphasises children's protection and professional services boundaries rather than discrimination prevention.

Florida's 2024 legislation established AI transparency requirements for government systems and mandated disclosures when AI creates or modifies political advertising, addressing deepfake concerns in elections. Under the FDBR, consumers can opt out of profiling that produces legal or similarly significant effects, addressing AI-driven automated decision-making in contexts like credit decisions, insurance underwriting, employment screening and access to essential services.

Industry-Specific Implications

Healthcare

Healthcare companies face the most immediate compliance pressure. Beyond CHINA Prevention Unit scrutiny, healthcare entities must navigate HIPAA requirements, state breach notification laws and potential AI regulation affecting telehealth and mental health applications. Foreign-owned companies or those transferring data internationally should expect enforcement attention in 2026.

Companies collecting biometric data, genetic information or detailed demographic profiles should conduct comprehensive risk assessments. Key evaluation points include documenting corporate ownership structures to identify foreign investors or parent companies, mapping data flows to determine whether health information crosses international borders, reviewing cloud service provider arrangements and data storage locations, and assessing whether business partnerships with foreign entities create exposure under the CHINA Prevention Unit's mandate. Additionally, Florida law restricts state and local government contracts with entities owned or controlled by foreign countries of concern, creating further compliance considerations for foreign-owned healthcare companies seeking government contracts or partnerships. Healthcare companies should also evaluate whether their data security practices meet the "reasonable measures" standard under Florida law, particularly for cross-border transfers.

Fintech and financial services

Financial services firms generally remain outside the FDBR's scope but face sectoral regulations under the Gramm-Leach-Bliley Act. However, fintech companies with foreign investment and those collecting health or biometric data for insurance or lending decisions should assess CHINA Prevention Unit exposure. Foreign-owned fintech companies should also note that, effective 1 July 2025, Florida law prohibits governmental entities from contracting with companies owned or controlled by countries of concern if such contracts involve access to personal identifying information. The intersection of financial services and healthcare data creates potential vulnerability. Companies processing payment data internationally should evaluate whether their ownership structures and data flows create compliance risks.

Education technology

Educational technology companies must consider how SB 482's parental control requirements would affect learning platforms using AI tutoring or assessment tools. Ed tech companies should monitor interactions with student privacy law and AI transparency requirements, particularly regarding algorithmic decision-making in admissions, placement or disciplinary contexts.

Telecommunications

Telecommunications providers typically fall outside the FDBR's scope but remain subject to data breach notification and security requirements. However, telecoms companies with foreign ownership or those offering health-related services through their platforms should evaluate CHINA Prevention Unit implications. As 5G networks enable more healthcare applications, the line between telecommunications and healthcare data collection becomes more blurred.

Data Breach Notification and Security Requirements

FIPA continues to impose notification obligations when breaches create a risk of financial harm. The statute's risk-based approach requires covered entities to investigate breaches and consult with relevant law enforcement agencies before determining whether notification is necessary. If after investigation and consultation the entity reasonably determines that the

breach will not cause financial harm to affected individuals, notification may be avoided. However, this determination must be reasonable, documented in writing, maintained for five years and provided to the Department within 30 days of the determination.

For breaches affecting 500 or more Florida residents, entities must notify the Department within 30 days of determining that a breach has occurred. If more than 1,000 residents are affected, entities must also notify all nationwide consumer reporting agencies. The notification to the Department must include specific information about the breach, the number of individuals affected and steps taken to address the incident. Third-party agents that maintain personal information on behalf of another entity must notify that entity as expeditiously as practicable but no later than ten days following determination of a breach or reason to believe a breach occurred.

Penalties can reach USD500,000 per breach, assessed at USD1,000 daily for the first 30 days, then USD50,000 per 30-day period up to 180 days. Notably, penalties apply per breach rather than per individual, creating more predictable liability than per-record penalty structures. The statute requires reasonable security measures to protect personal information and mandates secure disposal of records no longer needed for business purposes. The CHINA Prevention Unit's focus on foreign-owned healthcare companies suggests security practices will face particular scrutiny where cross-border data transfers occur.

Florida's State Cybersecurity Act requires state agencies to implement cybersecurity measures aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, including risk assessments, incident response protocols and mandatory reporting of cybersecurity incidents and ransomware attacks. While these requirements apply to government entities rather than private businesses, they signal the state's overall approach to data security and may influence expectations for reasonable security measures under the breach notification statute.

Looking Ahead

Florida's privacy landscape in 2026 reflects targeted enforcement rather than comprehensive regulation. The CHINA Prevention Unit's creation signals aggressive action on foreign ownership concerns, particularly in healthcare. The potential passage of SB 482 would establish substantial AI governance requirements focused on protecting minors and preventing unauthorised professional services through automated systems. The Roku enforcement action demonstrates that Big Tech companies subject to the FDBR should expect active enforcement with regard to protection of children's data, transparency obligations and consumer opt-out rights.

This approach contrasts sharply with comprehensive privacy laws in California, Virginia, Colorado and other states. By focusing on specific perceived harms rather than establishing broad privacy frameworks, Florida is testing whether targeted, issue-specific regulation can protect consumers while minimising compliance burdens on most businesses. Florida's model mirrors broader state-level scepticism about foreign access to data and the risks posed by generative AI, reflecting national political dynamics around data sovereignty and technological competition with adversary nations. The model appeals to business interests by limiting regulatory obligations for the vast majority of companies while addressing concerns about data practices by dominant platforms, data collection by foreign entities and AI risks to children.

Florida's narrow model could face pressure to evolve if federal privacy or AI legislation advances in 2026–2027. Congressional proposals for comprehensive federal privacy legislation would pre-empt some state laws, though the extent of pre-emption remains contested. Federal AI regulation focusing on algorithmic discrimination, transparency or safety could establish baseline requirements that affect Florida's enforcement priorities. Additionally, if other states adopt more comprehensive frameworks and businesses seek regulatory harmonisation, Florida may face pressure to align with emerging national standards.

The practical impact of Florida's approach will depend significantly on enforcement intensity. The CHINA Prevention Unit's success in pursuing foreign-owned healthcare companies will determine whether other states adopt similar strategies. SB 482's passage and implementation will demonstrate whether targeted AI regulation focused on children and professional services can effectively address AI risks without comprehensive algorithmic governance frameworks. The Roku case and subsequent FDBR enforcement actions will establish whether Florida can effectively regulate Big Tech platforms while exempting mid-market businesses.

Healthcare companies with foreign ownership, Big Tech platforms under the FDBR, and any company deploying AI systems that interact with Florida children should prioritise compliance preparation in 2026. For these entities, Florida's targeted enforcement creates significant liability risk despite the state's generally business-friendly reputation. For most other businesses, Florida's light-touch approach means privacy obligations remain limited to breach notification and reasonable security measures rather than comprehensive privacy programme requirements. This dual reality (intense scrutiny for some, minimal obligations for most) defines Florida's distinctive privacy law landscape. Florida's 2026 enforcement and legislative activity will shape whether the state maintains its targeted model or moves toward broader privacy legislation in 2027.

USA – GEORGIA



Trends and Developments

Contributed by:

Jason Loring, Andrew Lee and Lara Sevenser
Jones Walker LLP

Jones Walker LLP has a privacy, data strategy and artificial intelligence team that helps clients with a full spectrum of data privacy, data protection and AI solutions, including identifying, preventing and responding to data incidents, contracting and transactional support, emerging technology guidance, and litigation and dispute resolution, all while managing and mitigating related risks. Its interdisciplinary team brings together highly experienced attorneys with professional backgrounds in a wide range of industries, including banking and financial services, health-

care, technology, telecommunications, energy, petrochemical, maritime, consulting, government, digital commerce and retail. Staying on top of legal, compliance and regulatory obligations under the myriad of burgeoning global privacy, data protection, and AI-related laws, regulations, frameworks and standards can be challenging for any organisation, large or small. Jones Walker has the knowledge and practical experience to help clients navigate these laws, obligations frameworks and standards. Timely insights can be found at www.AILawBlog.com.

Authors



Jason Loring is a partner in the corporate practice at Jones Walker and co-leads the firm's privacy, data strategy and artificial intelligence team. He advises clients on data privacy and protection, cybersecurity,

data governance, breach response, data strategy, and AI and machine learning, as well as strategic technology transactions and related commercial matters. Jason focuses his practice on data privacy, data protection, cybersecurity, AI adoption, deployment, and risk mitigation, privacy assessments and audits, data innovation, incident response and proactive incident readiness, vendor and outsourcing agreements and contracts, and related legal and regulatory matters.



Andrew Lee founded and serves as co-leader of Jones Walker's privacy, data strategy and artificial intelligence team and holds the CIPP/US designation from the International Association of Privacy Professionals.

Andy also chairs the firm's innovation committee and co-leads the technology industry team. Andy's data privacy and security work involves advising clients in the areas of data privacy and cybersecurity resilience and recovery. He helps develop,

implement and enforce policies and procedures to ensure defensible, repeatable and efficient processes and programmes related to the security of sensitive corporate data, recovery after cyber intrusions, litigation defence and prosecution, and complex electronic discovery of data in legal proceedings and internal investigations.



Lara Sevenser is a partner in the corporate practice group and co-leader of the technology industry team at Jones Walker. Lara's practice focuses on advising clients with respect to strategic commercial

contracting as well as drafting and negotiating complex technology, outsourcing and digital transactions. She has represented international and domestic businesses, including publicly traded corporations, privately held companies, utilities and partnerships in multimillion-dollar transactions domestically and globally. She regularly advises on the use, licensing, acquisition and commercialisation of intellectual property, including matters regarding privacy and data protection. Prior to joining Jones Walker, Lara served as global lead procurement, technology and outsourcing counsel for a leading global audit and consulting organisation.

Jones Walker LLP

1221 Peachtree Street, N.E.,
Suite 400
Atlanta, Georgia 30361
USA

Tel: +1 404 870 7531
Email: jloring@joneswalker.com
Web: www.joneswalker.com



Georgia's Privacy Landscape: Operating Without a Comprehensive Framework

As comprehensive data privacy laws proliferate across the United States, Georgia has not enacted one, despite sustained legislative efforts in the 2024 and 2025 sessions that continue in 2026. Georgia's most ambitious privacy law, the Protecting Georgia's Children on Social Media Act (SB 351), was signed into law in 2024 but later blocked by a federal court just days before its July 2025 effective date. Meanwhile, Georgia's courts have been developing common law doctrine imposing data protection obligations on organisations in the absence of a statute requiring them.

While Georgia has no omnibus consumer privacy statute, organisations operating in the state are not without obligations. The state's breach notification law applies; evolving common law duties are being established through litigation; federal sectoral regimes govern healthcare, financial and educational data; and the state attorney general's (AG) office has maintained an active enforcement posture. For practitioners advising clients with Georgia operations, this convergence of legislative inaction and legal developments across all three branches of government creates a compliance environment that is more demanding than it might initially appear. This article examines the key developments: the repeated failure of comprehensive consumer privacy legislation, the constitutional litigation over children's social media, a landmark common law data breach ruling, the courts' first encounter with AI-generated legal fabrication, and the state AG's enforcement activity.

Comprehensive privacy legislation: two sessions, no law

Georgia remains one of the largest states by population and economic output, yet lacks a comprehensive consumer data privacy statute. The General Assembly advanced such legislation in each of the past two annual sessions, each time falling short in a pattern reflecting sustained tension between a Republican-majority Senate committed to a business-friendly framework modelled after Virginia's, and a House unwilling to pass it in that form.

SB 473 (2024)

The Georgia Consumer Privacy Protection Act (SB 473) passed the Senate on 27 February 2024, by a vote of 37–15 and was favourably reported by the House Technology and Infrastructure Innovation Committee on 20 March 2024. The legislature adjourned in late March without a House floor vote, however, and the bill died without becoming law.

SB 473 drew sustained criticism from consumer advocates. The Electronic Privacy Information Center (EPIC) assigned it an "F" grade, and the American Civil Liberties Union (ACLU) of Georgia characterised it as protecting technology companies rather than Georgia residents. The critiques focused on high applicability thresholds limiting coverage, enforcement that was limited to the AG with no private right of action, and provisions that arguably favoured data industry interests over consumer rights. The bill would have applied to entities exceeding USD25 million in annual revenue that either (i) processed data of at least 175,000 Georgia residents, or (ii) processed data of at least 25,000 residents while deriving more than 50% of gross revenue from data sales. Civil penal-

ties ran up to USD7,500 per violation with a 60-day cure period. A notable affirmative defence applied to entities whose privacy programmes conformed to the National Institute of Standards and Technology (NIST) Privacy Framework. Whether NIST alignment would carry persuasive weight in a common law negligence action is a separate and open question. Like other Virginia-model bills, SB 473 excluded employment and business-to-business data from its “consumer” definition, a significant limitation for employers and commercial data operators.

SB 111 (2025)

The 2025 session brought Senate Bill 111, a substantially similar measure. It passed the Senate on 3 March 2025, by 53–2 and crossed to the House before the 6 March crossover deadline. EPIC again assigned a failing grade; the ACLU of Georgia told a House committee the legislature would be “voting in favour of the worst consumer protection act in the country”. The House withdrew and recommitted the bill on 27 March 2025, and comprehensive privacy legislation died a second time when the General Assembly adjourned on 4 April 2025. Whether sponsors will revive SB 111, negotiate amendments or introduce a successor measure is among the most closely watched questions in Georgia privacy law in this first quarter of 2026.

Implications for organisations

These failures do not leave organisations without data protection obligations in Georgia. The state’s breach notification statute applies; Georgia courts are actively developing common law data protection standards; and federal sectoral regimes – the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act apply regardless of the state-law void. Multistate businesses must implement consumer rights mechanisms for California, Virginia, Colorado and other regulated states regardless of Georgia’s posture. The structure of any 2026 successor legislation will shape compliance obligations for healthcare systems, insurers and banks. The critical question is scope: will lawmakers exempt HIPAA-covered entities and GLBA-regulated financial institutions from the statute entirely, or will they adopt narrower carve-outs that protect only regulated data while

leaving other AI-related activities subject to the new law? Organisations in those sectors should track the exemption architecture closely.

SB 351 and the Constitutional battle over children’s social media

While comprehensive privacy legislation stalled, Georgia enacted one of the nation’s most significant children’s online safety statutes. Governor Brian Kemp signed SB 351 (the Protecting Georgia’s Children on Social Media Act of 2024) on 23 April 2024, to be effective 1 July 2025. The law requires social media platforms to make commercially reasonable efforts to verify the age of account holders and to refuse account services to minors without parental consent. On advertising and data collection, the law is specific: platforms may not display advertising in a minor’s account based on personal information (with age and location as the sole permitted exceptions) and must limit collection and use of personal information from minor accounts to what is adequate, relevant and reasonably necessary for disclosed purposes.

The law also imposes K–12 school obligations on two tracks. Local governing bodies were required to adopt acceptable-use policies covering student access to obscene materials and content harmful to minors on school equipment by 1 October 2025, and adopt separate social media policies prohibiting student access to social media platforms on school-owned equipment (except under supervised educational use) by 1 April 2026. The State Board of Education could withhold state funding from non-compliant governing bodies. A separate civil liability provision creates damages exposure for commercial entities that distribute material harmful to minors on public websites without performing reasonable age verification, with fines up to USD10,000 per violation; internet service providers, cloud service providers and news-gathering organisations are exempt. Enforcement of the platform-facing requirements rests exclusively with the AG, who may seek damages of up to USD2,500 per violation following a 90-day cure period; there is no private right of action.

The preliminary injunction

On 26 June 2025, just five days before SB 351’s implementation date, Judge Amy Totenberg of the Northern

District of Georgia granted a motion for a preliminary injunction blocking enforcement of the law's core platform provisions (*NetChoice v Carr*, 789 F. Supp. 3d 1200 (N.D. Ga. 2025)). The case has emerged as a leading decision on the constitutionality of state social media age restrictions. NetChoice, whose members include major online platforms, has challenged similar laws across the country; only Tennessee's survived a preliminary injunction motion, and only on irreparable harm grounds rather than First Amendment merits.

Judge Totenberg held that SB 351 was unconstitutional on its face. The law's "primary downfall", she wrote, was that it created a content-based restriction by distinguishing between platforms hosting user-generated content and those publishing provider-generated content, applying its requirements to the former while exempting the latter. The court's illustrations are pointed: SB 351 would apply to a user posting news on X but not to the New York Times posting to its own liveblog; it would cover the Georgia Bulldogs Reddit forum but not Barstool Sports. That asymmetry triggered strict scrutiny, which the law failed. The court further found that the law burdened anonymous speech for all Georgians by conditioning access to major digital public forums on the provision of government identification, and that the age verification requirements created an independent chilling effect by forcing collection and storage of sensitive personal information (notably, while the act requires deletion of parental consent data after verification, no comparable deletion obligation applies to the broader age verification data collected from users). "Because of the enormous burdens imposed on the First Amendment rights of children, adults, and social media platforms", Judge Totenberg wrote, "even the state's serious interest here cannot justify SB 351 under the First Amendment's rigorous standards". The court was explicit that the deficiency was one of constitutional tailoring, not legislative purpose. District court proceedings have been administratively closed pending the interlocutory appeal, which Georgia filed on 17 July 2025.

The appeal and Free Speech Coalition v Paxton

The day after Judge Totenberg's ruling, the US Supreme Court decided *Free Speech Coalition, Inc. v Paxton*, 606 U.S. 461 (2025), upholding Texas's

age-verification law for websites whose content is predominantly sexually explicit material harmful to minors under intermediate scrutiny. *Paxton*, however, does not map cleanly onto SB 351. The Texas law targeted sites where more than one-third of content is sexually explicit material already categorically unprotected as to minors and was specifically structured to require age verification without retention of users' identifying information. SB 351 regulates broad-based social media platforms hosting constitutionally protected speech across an unlimited range of subjects. Whether *Paxton*'s intermediate scrutiny framework extends to general-purpose social media regulation is a question the Supreme Court specifically declined to resolve. Legal commentators are divided, making the US Court of Appeals for the Eleventh Circuit's decision genuinely uncertain and nationally significant.

Pending the appeal, SB 351's platform-facing requirements remain unenforceable. Social media companies should audit age-assurance capabilities and monitor the docket closely, as a reversal could impose substantial obligations on short notice. The school-level obligations present a different picture: tied to state funding compliance rather than First Amendment platform restrictions, those requirements have been advancing on a separate compliance track. The 1 October 2025 acceptable-use policy deadline has passed; school districts should now be focused on the 1 April 2026, social media policy deadline, which remains operative regardless of the platform injunction's status. School district counsel should not assume the Eleventh Circuit appeal relieves district obligations under SB 351's K–12 provisions.

Data breach liability: common law takes shape

The most consequential Georgia privacy ruling of 2025 came in October, when the Court of Appeals decided *Bland v Urology of Greater Atlanta, LLC*, 377 Ga. App. 177 (Ga. Ct. App. 2025), the first Georgia appellate decision to recognise a common law duty of care to protect personally identifiable information against foreseeable cybersecurity risks.

The case arose from a breach at a Georgia medical practice. Plaintiffs filed a putative class action alleging negligence, breach of implied contract, and related claims after their personal information (including

Social Security numbers, dates of birth, addresses and health insurance details) was exfiltrated and appeared for sale on the dark web. The trial court dismissed the complaint in full. Presiding Judge Christopher McFadden, writing for a unanimous panel, reversed on the negligence, implied contract and implied covenant claims while affirming dismissal with prejudice of the unjust enrichment claim on the ground that plaintiffs failed to allege the defendant received any benefit from their personal information. On the duty-of-care question (a matter of first impression for Georgia appellate courts), the panel looked to the Eleventh Circuit's analysis in *Ramirez v The Paradise Shops*, 69 F.4th 1213 (11th Cir. 2023) (persuasive, not binding), concluding that the foreseeability of medical identity theft, combined with the defendant's ability to prevent the breach through reasonable measures, established a duty at the pleading stage.

On injury, the court held that plaintiffs adequately alleged harm by claiming their personally identifiable information had been stolen and offered for sale on the dark web, and that an imminent fraud risk followed, aligning Georgia state doctrine with *Ramirez*'s standing analysis, which treated imminent misuse of stolen data as sufficient injury. *Bland* did not definitively resolve the standing issue where data was accessed but not yet demonstrably misused; that argument remains available to defendants as the doctrine develops. The implied contract holding adds a second avenue for plaintiffs: the exchange of personal information as a condition of receiving services or employment creates contractual obligations to protect that information.

Bland changes the litigation risk calculus for Georgia organisations holding significant volumes of sensitive personal information (particularly healthcare providers) by applying traditional tort foreseeability principles to data breach liability for the first time at the Georgia appellate level. The decision provides no guidance on which security measures will satisfy the duty at the merits stage, leaving organisations to calibrate investments against data sensitivity, breach likelihood and evolving industry standards. Counsel should review incident response plans, cybersecurity documentation and data governance practices accordingly. Post-*Bland*, the breach notification framework and com-

mon law liability require integrated analysis: a breach triggering statutory notification obligations will generate facts directly relevant to negligence and implied contract claims, and organisations should not manage these exposures in separate tracks.

AI in the courts: hallucinations, sanctions and practitioner accountability

Georgia's courts confronted AI-generated legal hallucinations for the first time in June 2025. In *Shahid v Esaam*, 376 Ga. App. 145 (Ct. App. June 30, 2025), the Court of Appeals vacated a trial court order and imposed the maximum available sanctions after finding that counsel had submitted briefs containing fabricated case citations likely generated by AI. The trial court's denial order itself cited two non-existent cases originating in the opposing attorney's filings. On appeal, that attorney submitted a brief containing 11 additional fabricated citations out of 15 total, including a fictitious 2009 Georgia Supreme Court case cited in support of an attorney's fees request. The Court of Appeals imposed a USD2,500 sanctions award (the maximum permitted) and vacated the trial court order for relying on non-existent authority.

The court used the occasion to place Georgia's legal profession on broad notice. Citing US Supreme Court Chief Justice John Roberts's 2023 Year-End Report on the Federal Judiciary and similar incidents in other jurisdictions, it catalogued the systemic harms: wasted resources for courts and opposing parties, reputational injury to judges whose names appear on fabricated opinions and, most critically, the risk that decisions rest on non-existent law. For privacy and technology practices specifically, *Shahid* signals that Georgia courts will treat hallucinated citations as sanctionable professional conduct, not harmless error. Practitioners should monitor local circuit rules as Georgia courts may develop formal AI disclosure requirements through additional sanctions decisions, standing orders or court rules. Independent citation verification should be treated as a core professional obligation, not a precautionary option.

Data breach notification: framework and recent incidents

Georgia's data breach notification statute, the Personal Identity Protection Act, Ga. Code Ann. §§ 10-1-

910 et seq., requires information brokers and data collectors to notify affected Georgia residents following discovery of a breach involving unencrypted personal information that was, or is reasonably believed to have been, acquired by an unauthorised person. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with law enforcement needs or measures necessary to determine the scope of the breach and restore the integrity of the data system. Unlike most state breach statutes, Georgia's imposes no fixed notification deadline.

Two additional provisions warrant particular attention from compliance and incident-response counsel. First, third-party data processors maintaining personal information on behalf of a covered entity must notify the data owner within 24 hours of discovering a breach, a tight window demanding advance planning and contractual clarity in vendor agreements. Second, when notification is required for more than 10,000 Georgia residents at one time, the notifying entity must also notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices without unreasonable delay. One common point of confusion warrants clarification: Georgia's statute does not impose a "substantial harm" trigger. The notification obligation arises upon unauthorised acquisition of the covered data, without any harm-probability filter; organisations cannot use a harm assessment to avoid notification when covered personal information has been accessed without authorisation.

The Dublin Medical Center breach illustrates the persistent vulnerability of smaller healthcare providers. Suspicious activity was detected on 17 October 2025; forensic investigation confirmed unauthorised access and potential exfiltration of patient data affecting 32,090 patients, as reported to the US Department of Health and Human Services' Office for Civil Rights. Notification letters began mailing on 17 December 2025, and plaintiffs' counsel announced class action investigations in January 2026. Following Bland, smaller practices and regional systems with limited cybersecurity resources face the combination of HIPAA enforcement exposure, Georgia breach notification obligations, and expanded common law tort liability, a convergence that makes proactive

investment in incident response planning increasingly urgent.

Attorney General Carr: enforcement, advocacy and the FBPA

Georgia AG Chris Carr has maintained an active profile on data privacy and children's online safety across enforcement, litigation and federal legislative advocacy. On the federal front, Carr joined 31 other attorneys general in a late-2024 letter to congressional leadership urging passage of the Kids Online Safety Act (KOSA). In February 2026, he joined a coalition of 40 state and territorial AGs urging Congress to advance the Senate version of KOSA (S. 1748) while rejecting a House version the coalition viewed as insufficiently protective. That same month, AG Carr's office opened a civil investigative demand inquiry into Roblox Corporation, seeking information about the platform's safety practices for minors, illustrating a regulatory strategy visible in AG offices nationally: deploying investigative authority proactively in the absence of comprehensive enforcement statutes.

A frequently overlooked dimension of Georgia's enforcement landscape is the AG's authority under the Georgia Fair Business Practices Act (FBPA), Ga. Code Ann. §§ 10-1-390 et seq., the state's primary unfair or deceptive acts or practices (UDAP) statute. The FBPA broadly prohibits unfair or deceptive practices in the unregulated consumer marketplace (it does not extend to areas already governed by other state or federal regulatory frameworks) and empowers the AG to investigate, seek injunctive relief, impose civil penalties, and require restitution. Although the UDAP does not expressly address data privacy, AGs in Georgia and nationally have used analogous UDAP authority against entities whose data practices involve misleading privacy disclosures, inadequate security representations or deceptive data-sharing conduct. Organisations that make public commitments about their data practices (through privacy notices, marketing materials or terms of service) and fail to honour them face FBPA exposure in addition to breach notification and common law liability. Privacy counsel should audit external-facing data representations for consistency with actual organisational practices. The combination of SB 351 litigation, multistate coalition advocacy, targeted platform investigations and FBPA

enforcement authority constitutes a multifaceted posture unlikely to diminish.

Looking ahead

The 2026 Georgia legislative session presents another opportunity to enact comprehensive consumer privacy legislation. The structural conditions have not fundamentally shifted: the Senate's institutional commitment to a Virginia-model framework remains strong and the House's resistance equally persistent. Any path to enactment likely requires targeted amendments to applicability thresholds and consumer rights provisions or a political catalyst (eg, federal action, a high-profile Georgia breach or continued regional competitive pressure) sufficient to break the impasse. Whether sponsors revive SB 111 or introduce a successor measure is itself an early indicator worth watching.

The Eleventh Circuit's decision in *NetChoice v Carr* will likely be among the most consequential privacy law developments of 2026 for Georgia and the nation. Reversal, finding that *Free Speech Coalition v Paxton*'s intermediate scrutiny framework extends to broad-based social media regulation, would activate SB 351's requirements on relatively short notice. Affirmance would shift attention to whether Georgia's constitutional defects can be remedied through narrower drafting or whether the challenge is more fundamental. The common law framework established by *Bland* will continue developing through trial court and appellate decisions; as subsequent cases reach the Court of Appeals, the merits-stage contours of reasonable security, injury and causation will become clearer, with significant consequences for litigation strategy, cybersecurity investment decisions and insurance pricing. The judicial and professional response to AI in legal proceedings, initiated by *Shahid*, is also likely to develop further through additional sanctions decisions, court rules or advisory opinions; privacy and technology practitioners should treat it as the opening chapter of a longer conversation.

Conclusion

Georgia's privacy landscape in early 2026 is defined by intersecting legal contests across all three branches of government. The repeated failure of comprehensive legislation, the constitutional battle over SB 351, the emergence of common law breach liability, the judiciary's first encounter with AI fabrications and the AG's expansive enforcement posture each demand attention from practitioners advising clients with Georgia operations, and none can be understood in isolation.

The central message for data protection professionals is that the absence of legislation does not mean regulatory relief. Georgia imposes breach notification requirements, evolving common law standards and federal sectoral obligations, and its AG is using existing enforcement tools aggressively in the interim. Georgia's posture also stands in growing contrast to that of its immediate neighbours: Florida enacted a comprehensive consumer privacy law in 2023, Tennessee enacted one in 2024 and North Carolina is among the states actively advancing comprehensive legislation. As more Southeast states establish statutory frameworks, Georgia businesses will face those obligations across state lines while their home-state framework remains unsettled. Organisations serious about managing their Georgia privacy exposure should invest in proactive programme design now, without waiting for legislative clarity that may not arrive on any predictable schedule.

USA – ILLINOIS



Trends and Developments

Contributed by:

Paul Yovanic, Jason Priebe, Ada Dolph and Michael Jacobsen
Seyfarth Shaw LLP

Seyfarth Shaw LLP and its DATA (Digital Asset and Technology Advocacy) Law practice helps clients manage data-driven legal risk while supporting their strategic business objectives. The practice integrates privacy, information governance, eDiscovery, data science and analytics, cybersecurity, and AI advisory into a single, co-ordinated approach, allowing clients to address complex data issues without fragmented legal advice. The firm advises clients across the full data life cycle, including global privacy compliance, litigation and investigation readiness, defensible governance and eDiscovery strategies, cyber-incident response, and the legal implications of emerging

technologies such as artificial intelligence. Seyfarth supports both proactive risk management and high-stakes disputes, delivering practical, scalable solutions that adapt to evolving regulatory and technological environments. With experience across highly regulated and innovation-driven industries – including financial services, healthcare, life sciences, retail and advanced manufacturing – Seyfarth’s DATA Law practitioners assist clients ranging from emerging companies to multinational enterprises, and provide cohesive legal strategies that reduce risk and enable responsible, effective use of data.

Authors



Paul Yovanic is a nationally recognised partner in Seyfarth Shaw’s litigation department and a member of the firm’s DATA Law practice. He focuses on class actions – particularly data privacy and information security

cases – including defending clients in data breach litigation and suits under the Illinois Biometric Privacy Act (BIPA), the Illinois Genetic Information Privacy Act (GIPA) and the California Invasion of Privacy Act (CIPA). Paul frequently handles high-profile, first-impression matters and advises on biometric technology risk and compliance. He writes and speaks on emerging privacy issues, co-edits Seyfarth’s Consumer Class Action Defense Blog, and serves as a panelist at various thought-leadership conferences.



Jason Priebe is a partner in Seyfarth Shaw’s data law group and associate general counsel for the firm. He is an authority on data privacy, cybersecurity and eDiscovery. He advises clients on compliance, risk

management and litigation, focusing on GDPR, CCPA, cross-border data transfers and incident response. Jason helps businesses develop defensible data retention policies, mitigate privacy risks in vendor contracts, and navigate regulatory inquiries. He also counsels organisations on litigation holds, investigations and data breaches. Jason is a recognised authority on domestic and international privacy compliance, and routinely provides advice on the establishment of policies and procedures for electronic information management, controls, security and governance.

USA – ILLINOIS TRENDS AND DEVELOPMENTS

Contributed by: Paul Yovanic, Jason Priebe, Ada Dolph and Michael Jacobsen, **Seyfarth Shaw LLP**



Ada Dolph is a partner at Seyfarth Shaw with over 20 years' experience at the firm. She is a trusted adviser on biometric privacy, data protection and workplace privacy laws. She counsels clients on compliance with the Illinois

Biometric Information Privacy Act (BIPA), the Illinois Genetic Information Privacy Act (GIPA) and other evolving privacy regulations, helping businesses mitigate litigation risks and navigate complex data protection challenges. Ada defends companies in high-stakes BIPA class actions and other privacy-related disputes, leveraging her deep experience in employment and consumer privacy issues. She was lead counsel in the first BIPA case heard by the US Court of Appeals for the Seventh Circuit, resulting in a complete dismissal of the action.



Michael Jacobsen is a partner in Seyfarth Shaw's labour and employment department, and leads Seyfarth's Illinois Biometric Information Privacy Act (BIPA) class action team. He helps businesses

navigate the complexities of BIPA and other evolving privacy laws, providing strategic guidance on risk mitigation, policy development and statutory compliance. Michael defends clients in high-stakes BIPA litigation, and counsels them on best practices for biometric data collection and consent requirements. Clients rely on Michael's expertise to reach decisive, favourable resolutions early on in the matters he defends, as well as in the ongoing development of successful, long-term strategies both in and beyond litigation.

Seyfarth Shaw LLP

233 South Wacker Drive
Suite 8000
Chicago
Illinois 60606
USA

Tel: +1 312 460 5000
Fax: +1 312 460 7000
Email: pyovanic@seyfarth.com
Web: www.seyfarth.com



Illinois continues to stand at the forefront of US privacy law, and 2026 is shaping up to be one of its most consequential years yet. Following a period marked by rapidly expanding litigation under the Illinois Biometric Information Privacy Act (BIPA), the resurgence of the Illinois Genetic Information Privacy Act (GIPA) and new AI-focused regulation affecting employers state-wide, courts and regulators are poised to address several foundational questions that will define the future of privacy compliance and risk in the state. With key appellate decisions pending, courts deepening their divisions and newly enacted AI obligations introducing sweeping operational challenges, Illinois remains a critical – and increasingly complex – jurisdiction for organisations navigating biometric, genetic and automated decision-making rules. This article explores the pivotal developments shaping that landscape and the implications for businesses operating in or connected to Illinois.

The Illinois Biometric Information Privacy Act (BIPA, 740 ILCS 14/ et seq)

Enacted in 2008, BIPA has long regulated the collection, use and handling of biometric identifiers and information by private entities, but for years it attracted relatively little litigation. That changed dramatically after the Illinois Supreme Court's 2019 decision in *Rosenbach v Six Flags Entertainment Corporation*, which held that plaintiffs need not allege actual harm to pursue statutory damages under BIPA. In the wake of *Rosenbach*, filings surged – now exceeding 1,500 cases – and courts at every level have been pressed to address foundational questions about the scope and operation of the statute.

In the authors' 2025 Trends and Developments update, they highlighted three issues that were rising to the forefront at that time:

- the applicability of BIPA's healthcare exemption to employee time-clock scans;
- the reach of the state-contractor exemption under BIPA; and
- whether the 2024 amendment limiting damages to a single recovery applies retroactively to cases that were pending when the amendment took effect.

Going into 2026, there has been significant movement with respect to the state-contractor exemption and the retroactivity of the statutory damages amendment – both in state court and in federal court – setting the stage for pivotal developments on both of these fronts.

State-contractor exemption

BIPA contains an often-overlooked provision exempting any “contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government”. Historically, the only Illinois appellate decision interpreting that language has been *Enriquez v Navy Pier, Inc*, where the First District established a three-part framework for applying the exemption: the entity seeking to avail itself of the exemption must have been a contractor, of a governmental unit, and working for that governmental unit at the time of the alleged biometric collection. Focusing on the ordinary meaning of the statutory text, the court held that the defendant in *Enriquez* fit comfortably within the exemption because it was performing services under a contract with a unit of government.

Despite the appellate court's straightforward approach in *Enriquez*, trial courts have continued to diverge in their approaches. Some – most notably in *Miranda v Pexco, LLC* – have adopted a strictly temporal view consistent with the court's plain reading in *Enriquez*, ruling that the exemption applies so long as the defendant held a government contract during the period that the plaintiff worked for the defendant, regardless of whether the biometric collection related to the governmental work. Other courts have expanded the inquiry, requiring discovery into the scope of the contract, the revenue derived from it, or the degree to which the alleged biometric collection was tied to governmental responsibilities, often deferring any ruling until summary judgment. As a result, the exemption continues to be one of the most inconsistently applied features of the statute.

Further important developments are expected in 2026. In January, the Third District heard oral arguments in a case that is expected to provide the first ruling on the exemption from an Illinois appellate court since *Enriquez*. Although the discussion in this

case touched on whether the exemption should turn on a functional nexus between the biometric activity and the governmental work, the appellate panel also explored the practicality and predictability of a more straightforward temporal framework – an approach that trial courts have already found to be more workable in its application. A written opinion has not yet been issued, but any guidance from the Third District will likely shape how courts state-wide evaluate the exemption and could help bring greater clarity to an area where a consistent, temporally focused analysis would provide both courts and litigants with a clearer path forward. Alternatively, should the Third District hold contrary to the First District, there is little doubt that the trial courts will continue to take inconsistent approaches themselves, and BIPA litigants will look to the Illinois Supreme Court for clarification.

At the same time, the state-contractor exemption is also drawing increased scrutiny in federal court. In late 2025, a Northern District of Illinois judge granted a motion for interlocutory appeal under 28 USC Section 1292 (b) after denying a defendant's attempt to invoke the exemption at the pleadings stage. Specifically, the question for interlocutory appeal is whether the state-contractor exemption imposes a purely temporal test or whether the BIPA violation must occur within the scope of a government contract. The court concluded that the question presents a controlling, unsettled issue of law appropriate for immediate appellate review. The matter was accepted by the Seventh Circuit for review, fully briefed, and oral arguments were heard in mid-February 2026.

Together, the pending Third District and Seventh Circuit decisions make 2026 a year to watch for the state-contractor exemption under BIPA. Until clearer guidance emerges, entities performing government-related work should continue to document their contractual roles and the nature of the work performed, as courts remain divided on whether the exemption turns on timing, function or some combination of both.

Retroactivity of statutory damages amendment

The question of whether the 2024 amendment to BIPA's damages provision applies retroactively remains one of the most unsettled – and consequen-

tial – issues in this space. The amendment, enacted in response to the Illinois Supreme Court's warning in *Cothron v White Castle System, Inc* that a per scan accrual theory could yield "potentially excessive damage awards", limits an individual to a single recovery for the same method of collection. Whether that limitation governs only post amendment lawsuits or also applies to cases based on conduct that occurred before the amendment went into effect has sharply divided courts.

When the authors last wrote about this, the federal courts were already split. That divide has since deepened and in some respects shifted. One notable development is the court's reversal of its previous position in *Gregg v Central Transport LLC*. In late 2024, this court had been one of the few to deem the amendment a mere clarification of existing statutory language, meaning that it should apply retroactively under Illinois precedent governing the issue. However, in March 2025, the same judge revisited the issue and reached the opposite conclusion. After examining the statutory text and its conflict with *Cothron's* interpretation of what constitutes a "violation", the court determined that the amendment substantively changed the statute and therefore could not be applied to conduct or lawsuits predating its enactment under Illinois law. This reversal both underscores the difficulty that courts face in distinguishing "statutory clarification" from "substantive change" and highlights how rapidly views on retroactivity have evolved.

At the same time, another federal court confronted the same question and concluded – consistent with much of the emerging authority – that the amendment is not retroactive. In that case, the court emphasised that determining whether an individual was injured once or hundreds of times goes to the substance of the right itself, squarely placing the amendment on the substantive side of Illinois' retroactivity framework. The court denied the defendant's attempt to limit damages to a single recovery and, recognising the significance of the issue, certified its order for interlocutory appeal. In late 2025, the Seventh Circuit agreed to review this matter and accepted the request for interlocutory appeal. In doing so, the Seventh Circuit further consolidated this issue with the state contractor exemption above, in an attempt to determine both issues at

the same time. As a result, the Seventh Circuit's pending decision will be the first federal appellate guidance on this question – guidance that could meaningfully shape the trajectory of pending and future BIPA cases.

As courts continue to reassess the retroactivity issue – and even reverse themselves, as in *Gregg* – the landscape remains in flux. Until the Seventh Circuit or the Illinois Supreme Court weighs in, litigants should expect continued inconsistency across trial courts, with high-stakes consequences for exposure and strategy.

The Illinois Genetic Information Privacy Act (GIPA, 410 ILCS 513/ et seq)

Enacted a decade before BIPA, GIPA remained largely dormant for years, though the landscape began changing considerably in 2023. Since then, more than 100 class actions have been filed, many targeting employers whose pre-employment forms, post-offer medical exams or onboarding processes allegedly solicited genetic information in violation of the statute. GIPA's core purpose has always been to protect individuals from discriminatory use or unauthorised disclosure of genetic information, and its definitions – harmonised with the Health Insurance Portability and Accountability Act (HIPAA) and the Genetic Information Nondiscrimination Act (GINA) – sweep far beyond laboratory DNA tests to include family medical history, requests for genetic services, and information related to genetic research participation. The statute prohibits requesting or using genetic information as a condition of employment and provides for liquidated damages of USD2,500 for each negligent violation and USD15,000 for each reckless or intentional violation.

To date, most GIPA litigation has focused on employment-related claims, particularly those arising from pre-employment physicals or questionnaires that allegedly probed into an applicant's family medical history. Courts have permitted claims to proceed past the pleading stage where allegations plausibly involved “genetic information” as defined under HIPAA and incorporated into GIPA; at the same time, some decisions have narrowed the scope of viable claims by distinguishing between enquiries about a plaintiff's personal medical condition – rather than familial conditions – or by finding Employment Retirement

Income Security Act of 1974 (ERISA) pre-emption in wellness-programme contexts. Plaintiffs have also pushed to broaden the statute's reach, bringing cases against genetic-testing companies and tech platforms based on tracking-pixel activity and other alleged disclosures of genetic-related data to third-party analytics tools.

Going into 2026, the most significant developments will centre on class certification and merit-based summary-judgment rulings – neither of which have courts yet addressed in a meaningful way, but both of which are expected this year. Several of the earliest-filed 2023 cases are now reaching the procedural point where class certification briefing is imminent. Based on the issues raised in those cases and the dynamics already visible in the litigation, courts are likely to scrutinise Federal Rule of Civil Procedure 23 (a) and 23 (b)(3) requirements closely. Plaintiffs will emphasise uniformity: standardised forms, common onboarding protocols and employer-wide practices that allegedly required disclosure of family medical history. Defendants, by contrast, will point to variations in how oral medical-exam questions were asked, differences across examiners, job sites and time periods, and the threshold questions of whether the information requested qualifies as “genetic information” at all – elements that cut against commonality and predominance.

Typicality and adequacy challenges are also expected, particularly where named plaintiffs underwent different screening processes or answered different medical enquiries than absent class members. Ascertainability concerns will likely be central as well; because many alleged violations involve oral exchanges during medical exams with no written record, identifying who was actually asked a family-history question may prove difficult.

On the merits, early summary judgment decisions will likely address several recurring questions:

- whether particular enquiries constitute “genetic information” under HIPAA's definitions;
- whether requests were truly made as a condition of employment;

- whether inadvertent or stray references fall within GIPA's prohibitions; and
- whether defences such as ERISA pre-emption, extraterritoriality, OSHA-driven compliance or consent/authorisation defeat liability.

Defendants are also expected to push arguments that the statutory scheme – like BIPA's – requires courts to apply discretion in awarding damages, particularly in cases involving large putative classes and minimal actual harm.

Altogether, 2026 is shaping up to be a pivotal year for GIPA litigation. With class certification and summary judgment decisions on the horizon, courts will finally begin resolving the threshold issues that have thus far only been previewed at the motion-to-dismiss stage. These rulings will determine not only the viability of the earliest GIPA cases but also the trajectory of the statute as a potential parallel to BIPA – or, alternatively, as a narrower, more context-specific privacy statute that resists broad class treatment.

Illinois Privacy Legislative Developments

At the outset of 2026, the Illinois legislature considered approximately seven bills addressing privacy and technology regulation. Notably, the proposed Illinois Personal Information Privacy Act failed to pass, leaving the state without a comprehensive privacy framework comparable to the California Consumer Privacy Act (CCPA) or the Virginia Data Protection Act (VDPA). That said, Illinois continues to pursue a targeted regulatory approach, focusing on discrete categories of sensitive information, as seen with BIPA and GIPA, as well as recent legislative efforts that have sought to regulate the collection and use of precise geolocation data (eg, SB 2121 and HB 3712).

Of particular significance for Illinois – and for employers operating locally and nationally with Illinois personnel or job applicants – are new restrictions governing the use of artificial intelligence (AI) in employment-related decision-making. Illinois now joins jurisdictions such as California, Colorado and New York City in imposing stringent requirements on AI-driven hiring, performance evaluation and job-related assessments.

Effective January 2026, House Bill 3773 amended the Illinois Human Rights Act to regulate AI use in employment contexts (Illinois Human Rights Act, 775 ILCS 5/2-102, 2026). The statute defines AI broadly, encompassing both generative AI (content creation) and predictive AI (tools generating scores, rankings, classifications or recommendations). Employers must provide written notice to applicants and employees whenever AI is utilised for decisions related to recruitment, hiring, promotion, training, discharge, discipline, tenure or other employment conditions.

The law also prohibits AI applications that result in discriminatory outcomes based on protected characteristics. While this prohibition is noteworthy, it largely reiterates existing anti-discrimination provisions under 775 ILCS 5/2-102.

The Illinois Department of Human Rights (IDHR) was granted authority to promulgate rules governing notice requirements, timing and delivery methods. However, the text of the IDHR draft regulations under consideration expands the statutory scope and requirements significantly.

For example, where the statute refers to AI “use”, the draft rules extend coverage to any AI that “influences or facilitates” an employment decision, even in the absence of automated decision-making. This interpretation potentially encompasses a wide array of applications, including generative AI tools used for drafting job postings.

There are also disclosure requirements in the draft rules. Under the proposed framework, employers must disclose:

- the name of each AI product, along with its developer and vendor;
- the employment decisions that the AI influences or facilitates;
- the purpose of the AI system and categories of personal data processed, described in practical terms;
- the job positions for which the AI is deployed;
- a designated point of contact for enquiries; and

- information regarding the right to request reasonable accommodation (effectively an opt-out mechanism).

According to the draft regulations, AI notices to personnel must be posted in multiple locations, including:

- the employee handbook;
- a conspicuous physical location where workplace notices are displayed;
- the employer's internal and external websites; and
- text of all job postings.

Employers must also update these disclosures within 30 days of adopting any new AI technology. As AI technology develops and evolves, it is easy to imagine significant hours being spent updating the Illinois disclosures in order to confirm that each publication version is current, and that the technology use and descriptions are correct – not to mention the creation and management of the alternative opt-out process.

The statute's explicit ban on using zip codes as proxies for protected characteristics reflects concerns about geographic segregation in Illinois. However, the law does not prohibit reliance on other location-based data, such as city or county identifiers, creating potential ambiguity. That said, employers would be well advised to avoid incorporating *any identifier or variable* into AI-driven decision-making intended for use as a proxy aligned with a protected class or identifying characteristic.

While the state's attempt at an omnibus privacy law to regulate all categories of "personal information" has essentially stalled, the recent regulations concerning the collection and processing of discrete categories of sensitive personal information and the use of AI in employment are worthy of close attention. The framework for the regulation of AI for employment and hiring emphasises transparency and anti-discrimination. However, the expansive interpretation proposed by the IDHR introduces operational complexity (and potentially a practical impossibility) for employers. Organisations should monitor rule-making developments closely and consider steering clear of the state for AI personnel technology deployment until specific requirements are sorted out.

USA – MISSOURI



Trends and Developments

Contributed by:

Mark Williams and Stefanie Brody
Sandberg, Phoenix & von Gontard, P.C.

Sandberg, Phoenix & von Gontard, P.C. is a full-service law firm with more than 200 attorneys practising across over 35 areas of law, including business litigation, transactional law, regulatory compliance, medical and professional malpractice, products liability, insurance defence, and wealth and estate planning.

Serving clients nationwide, the firm is particularly recognised for its strength as trusted local and regional counsel throughout Missouri, Southern Illinois and Kansas. The firm maintains offices in St Louis, Clayton, St Charles and Kansas City, Missouri; Edwardsville and O'Fallon, Illinois; and Gainesville, Florida.

Authors



Mark Williams is counsel in the business practice at Sandberg Phoenix, where he advises organisations on data privacy, cybersecurity and artificial intelligence (AI). His practice spans compliance

programme design, incident response, regulatory investigations and AI governance across frameworks including the CCPA, HIPAA, GDPR and CMMC. When breaches occur, Mark guides companies through forensic investigations, containment, regulatory reporting and litigation risk mitigation. He also counsels clients on the legal and operational dimensions of AI deployment, including governance structures, regulatory exposure and liability considerations. Mark is a Certified Information Privacy Professional (CIPP/US) and advises on both domestic and international compliance matters.



Stefanie Brody is an attorney at Sandberg Phoenix in St Louis who focuses on data privacy, cybersecurity and related regulatory issues. She is part of the firm's data, privacy and cybersecurity practice,

and brings a strong foundation in procedural law shaped by years of clerking at the Missouri Court of Appeals. Stefanie holds the Certified Information Privacy Professional (CIPP/US) credential from the International Association of Privacy Professionals, underscoring her commitment to data protection, AI governance and compliance strategies for clients navigating evolving privacy laws. She advises organisations on privacy regulatory challenges and risk mitigation strategies.

Sandberg Phoenix & von Gontard, P.C.

701 Market Street
Suite 600
St. Louis
Missouri 63101
USA

Tel: +1 314 231 3332
Fax: +1 314 241 7604
Email: sbrody@sandbergphoenix.com
Web: www.sandbergphoenix.com



SANDBERG PHOENIX

Background

Missouri does not have a comprehensive consumer privacy statute, and its consumers cannot demand that a business disclose, delete or stop selling their personal data as a matter of state statutory right. That does not mean, however, that Missouri is a privacy vacuum.

Missouri currently relies on a patchwork of sector-specific laws for its data privacy and protection regulation. These laws include a broadly worded consumer protection law known as the Missouri Merchandising Practices Act (MMPA) and industry-specific regulations, such as the newly enacted Insurance Data Security Act. In recent years, the Missouri Attorney General's Office has aggressively pursued data privacy and data security enforcement actions through the MMPA against some of the nation's largest technology and financial services companies.

The MMPA as Missouri's Privacy Enforcement Tool

The MMPA, codified at Section 407.020 et seq of the Missouri Revised Statutes, is often described as Missouri's "mini FTC Act". It declares unlawful "the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce".

Missouri courts have interpreted an "unfair practice" under the MMPA to be "unrestricted, all-encompassing and exceedingly broad". See *Ports Petroleum Co, Inc of Ohio v Nixon*, 37 S.W.3d 237, 240 (Mo. banc 2001). Critically, the MMPA does not require proof of intent to deceive. Defendants' conduct, not their intent, determines whether a violation has occurred. This objective standard makes the MMPA a potent tool for addressing privacy violations when a company may not have intended to cause harm but nonetheless engaged in practices that were deceptive or unfair.

The MMPA provides for both public and private enforcement:

- the *Attorney General* may seek injunctive relief, restitution, disgorgement of profits, civil penalties, and

recovery of investigative and prosecution costs under Section 407.100; and

- *private plaintiffs* who purchase or lease merchandise primarily for personal, family or household purposes may bring civil actions to recover actual damages, and courts have discretion to award punitive damages and attorneys' fees under Section 407.025.

Recent Attorney MMPA General Enforcement Actions

Tax preparation pixel litigation

In July 2023, the Missouri Attorney General sued H&R Block, TaxSlayer and TaxAct (Case No 2322-CC01433), alleging that the companies installed tracking pixels (specifically the Meta Pixel and related tools) on their online tax preparation platforms. The petition alleged that these pixels transmitted sensitive financial information to Meta, Google and other technology companies, including consumers' names, adjusted gross income, refund amounts, filing status, dependent information, and whether consumers visited pages related to particular types of income, deductions or tax credits. The Attorney General alleged that this data sharing occurred without consumers' knowledge or consent and in direct contradiction of the companies' privacy policies, which assured users that their personal information would be safeguarded. The petition asserted claims for misrepresentation, omission, deception and unfair practices under the MMPA.

Both TaxAct and TaxSlayer subsequently settled with the state. TaxAct resolved the matter in November 2023 for USD195,000 and agreed to modify its data-sharing capabilities. TaxSlayer settled on similar terms. Litigation against H&R Block continued in Jackson County as of the last available reporting.

Google location-tracking settlement

Missouri participated in a 40-state coalition that investigated Google for allegedly misleading users about location data collection. The investigation allegedly revealed that Google continued to track users' locations even when the "Location History" setting was turned off through a separate "Web & App Activity" setting. In November 2022, Google agreed to a historic USD391.5 million multistate settlement requiring

greater transparency regarding location data collection.

Blackbaud data breach settlement

In October 2023, the Attorney General participated in a settlement with software company Blackbaud related to a 2020 ransomware breach that exposed the personal, financial and health information of millions of consumers. The Attorney General alleged that Blackbaud committed unfair and deceptive practices under the MMPA by failing to implement reasonable data security measures and delaying notifying affected consumers. The multistate settlement totalled USD49.5 million.

Meta youth safety litigation

Missouri joined 33 states in October 2023 in suing Meta, alleging that Facebook and Instagram employed manipulative design features targeting young users. Among other things, the complaint alleged that Meta violated the Children's Online Privacy Protection Act (COPPA) by collecting data from users under 13 years of age without parental consent. The Missouri Attorney General alleged misrepresentation, deception, concealment and unfair practices under the MMPA.

Other Attorney General MMPA enforcement

Beyond filing MMPA enforcement lawsuits, the Missouri Attorney General has a powerful investigative tool at its disposal: the civil investigative demand (CID). Under Section 407.040 of the Missouri Revised Statutes, when it appears to the Attorney General that a person has engaged in or is engaging in any method, act, use, practice or solicitation declared unlawful under the MMPA – or when the Attorney General believes an investigation is in the public interest – the Attorney General may issue a CID requiring a person to appear and testify or to produce relevant documentary material or physical evidence. A CID functions similarly to an administrative subpoena and is a pre-litigation investigative mechanism.

The Attorney General's CID power is not unlimited. Both the statute and constitutional principles constrain the scope of any demand, and a business that receives a CID is not without recourse. A business may petition the court to set aside or limit a CID, and

such challenges can raise both statutory and constitutional arguments.

The Missouri Attorney General has also promulgated privacy-related regulations under the MMPA. Most recently, the Attorney General instituted an age verification regulation for websites containing sexually explicit material. The rule, 15 CSR 60-18.010 et seq, applies to any website, application or self-contained sexual content segment where a "substantial portion" – defined as 33% or more – of publicly available content is "pornographic for minors". It mandates that covered entities verify users' ages through one of several methods:

- digital identification, defined as information stored on a digital network that serves as proof of the identity of an individual;
- government-issued photo identification;
- a commercially reasonable method that relies on public or private transactional data to verify the age of the individual, such as records from mortgage, education and employment entities; or
- an equally effective alternative method approved by the Attorney General.

As implemented in other states, approved age verification methods may include facial analysis technology, where the user submits selfies from which an AI algorithm estimates whether the individual is over the age of 18.

The rule expressly prohibits covered entities from retaining personally identifying information after the verification process is complete, reflecting an awareness of the data privacy risks inherent in identity verification at scale. Some platforms have elected to geo-block Missouri users rather than comply with the new rule.

The Injury Hurdle: Why Private MMPA Claims Are So Difficult

While the Attorney General has wide latitude in bringing MMPA enforcement actions, private plaintiffs face a far more constrained counterpart, particularly with respect to the statute's damages requirements. Section 407.025 and associated case law require private plaintiffs to establish three elements:

- that the plaintiff acted as a reasonable consumer in light of all circumstances;
- that the unlawful method, act or practice would cause a reasonable person to enter into the transaction that resulted in damages; and
- that there are individual damages with “sufficiently definitive and objective evidence to allow the loss to be calculated with a reasonable degree of certainty”.

The first hurdle may result in dismissal early on at the pleading stage. Whether an alleged practice is likely to mislead a reasonable consumer is distinct from the heightened pleading standard for fraud claims, but it imposes a meaningful threshold that privacy plaintiffs must clear before reaching discovery or damages questions.

This last requirement – the “ascertainable loss” standard – is the central obstacle for privacy plaintiffs. Missouri courts have strictly applied this standard to require concrete, quantifiable evidence of monetary loss.

The implications for privacy cases are significant. Traditional privacy harms – such as lost time, anxiety, reputational risk, or the abstract diminution in the value of personal data – are inherently difficult to reduce to a dollar figure. A plaintiff whose browsing data was secretly shared with an advertising platform may feel genuinely violated, but that may not easily translate to provable loss under the MMPA.

Missouri courts have recognised the “benefit-of-the-bargain” rule as a viable damages theory in MMPA cases. Under this approach, damages are measured as the difference between the actual value of the property and its value as represented. In theory, a plaintiff could argue that a service promising data confidentiality was worth less than what was paid because the provider was secretly sharing data with third parties. However, this theory remains untested.

Taken together, the reasonable consumer and ascertainable loss requirements create formidable obstacles for establishing privacy harm under the MMPA. No Missouri court has yet sustained a private MMPA

claim arising from unauthorised data sharing, data breach or similar conduct.

In *Kuhns v Scottrade, Inc.*, 868 F.3d 711 (8th Cir. 2017), the Eighth Circuit affirmed the dismissal of MMPA claims brought by customers alleging that a brokerage firm failed to implement adequate data security measures and failed to discover and promptly notify customers of a data breach. The court noted that the MMPA requires the alleged unlawful act to occur in relation to a sale of merchandise and that it result in identifiable financial harm connected to the merchandising practice. The claims did not meet these requirements because the defendant did not sell data security services, but rather implemented security measures inducing customers to transfer their personal information in order to obtain its brokerage services. The decision underscores that businesses facing data breach litigation in Missouri may have viable defences under the MMPA’s merchandise and loss requirements, but it also highlights the importance of ensuring that representations about data security practices are accurate and not misleading.

As matters currently stand, the Missouri Attorney General – who faces none of the damages, pleading or standing constraints that burden private litigants – has been the primary enforcer of the MMPA in the data privacy space.

Missouri’s Wiretapping Law and the Online Tracking Frontier

Missouri is a one-party consent state as regards its wiretapping and electronic surveillance laws, Section 542.400 et seq of the Missouri Revised Statutes. This stands in contrast to “two-party” or “all-party” consent jurisdictions such as California and Florida, where all participants must consent for a recording to be lawful. The one-party consent framework means that, in most circumstances, businesses recording customer service calls or other communications face a less onerous legal standard in Missouri than they would in an all-party consent jurisdiction.

However, Missouri’s one-party consent rule comes with an important caveat. Under Missouri’s wiretapping statute, it is lawful for one party to a communication to intercept that communication only where the

interception is not carried out “for the purpose of committing any criminal or tortious act”. This “tortious purpose” exception is a distinctive feature of Missouri’s wiretapping statute and has emerged as a significant source of litigation risk in the online tracking context.

A growing number of plaintiffs across the country have brought wiretapping claims against companies that deploy online tracking technologies such as the Meta Pixel on their websites. The theory is straightforward: when a company embeds a tracking pixel that intercepts and transmits the contents of a user’s communications to a third party such as Facebook, the company has “intercepted” a “wire communication” within the meaning of the wiretapping statute.

This theory has gained traction in Missouri. In *Jane Doe v SSM Health Care Corporation*, No 2222-CC10014-01 (Mo. Cir. Ct. City of St Louis, filed 25 September 2024), the plaintiff alleged that SSM Health embedded Meta Pixel and Facebook’s Conversions API on its hospital websites and patient portal, which caused patients’ sensitive medical information – including search queries about medical conditions, doctor appointments and patient portal interactions – to be secretly transmitted to Facebook along with personally identifying information such as Facebook user IDs and IP addresses. The plaintiff asserted, among other claims, that SSM Health violated Missouri’s wiretapping statute by intercepting patients’ wire communications for the purpose of committing criminal and tortious acts, including invasion of privacy, breach of the fiduciary duty of confidentiality, and conversion of patients’ personal health information. While the parties settled in November 2025, the case notably survived a motion to dismiss, signalling that Missouri courts are willing to entertain wiretapping claims premised on deployment of online tracking technologies.

The implications are significant. Unlike the MMPA’s private right of action, which requires proof of ascertainable monetary loss, the Missouri wiretapping statute provides for statutory damages (liquidated damages computed at the rate of USD100 per day of violation or USD10,000, whichever is greater), punitive damages (for wilful or intentional violations) and attorneys’ fees. The question remains open as to whether Missouri’s wiretapping statute extends to data practices

such as pixel tracking, session replay technology, or the covert sharing of browsing data with third parties.

Other Privacy-Related Statutes

Although Missouri lacks a comprehensive privacy law, it has enacted several narrower statutes that touch on data protection, including the following under the Missouri Revised Statutes:

- Section 407.1355 prohibits the public posting or display of Social Security numbers, requires secure transmission of Social Security numbers over the internet, and bars employers from requiring employees to use their Social Security numbers as employee identification numbers;
- Section 407.433 restricts the disclosure of credit and debit card account numbers on sales receipts, prohibiting the display of more than the last five digits; and
- Section 362.422 mirrors federal Gramm-Leach-Bliley Act requirements to prohibit financial institutions from disclosing non-public personal information to non-affiliated third parties and requiring privacy notices to customers.

These provisions, while limited in scope, reflect a legislative awareness of specific data protection risks and should be accounted for in any Missouri-focused compliance programme.

Biometric Privacy

Missouri has not enacted a general biometric privacy statute. There is no Missouri law analogous to the Illinois Biometric Information Privacy Act, which has generated a wave of class action litigation in that state. Missouri businesses that collect fingerprints, facial geometry or other biometric identifiers are not subject to a standalone state law governing biometric data collection, consent, retention or destruction.

That said, Missouri does regulate biometric data in at least one narrow context. Section 313.817 (5), enacted as part of the state’s Licensed Gaming Activities framework, prohibits excursion gambling boats (known locally as riverboat casinos) from requiring patrons to provide fingerprints, retinal scans, biometric forms of identification, or patron-tracking cards as a condition of entry.

Businesses operating in Missouri should not assume that the absence of a general biometric privacy law eliminates risk entirely. The MMPA's broad prohibition against unfair and deceptive practices could apply to biometric data collection that is misleading or inadequately disclosed.

Healthcare Data Privacy

Healthcare data privacy is an area of evolving complexity in Missouri. Missouri has enacted a patchwork of state statutes protecting the confidentiality of specific categories of medical information. These include laws governing the confidentiality of HIV records (Section 191.656), genetic information (Section 375.1309), mental health records (Section 630.140), cancer registry data (Section 192.655) and newborn hearing screening results (Section 191.928). Abortion reports submitted to the Department of Health and Senior Services are also subject to confidentiality requirements under Section 188.070. These laws intersect with Missouri's unsettled legal landscape for reproductive and gender transition services, which present significant questions about the handling and reporting of sensitive health data for businesses in the healthcare sector, particularly when complying with the Attorney General's investigations into such services.

The Insurance Data Security Act – New Compliance Requirements

One of the most significant recent developments in Missouri's data privacy landscape is the Insurance Data Security Act, which took effect on 1 January 2026. This law establishes comprehensive data security standards for insurers, insurance producers and other licensed entities operating in the state. Missouri's enactment aligns the state with the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law, which has now been adopted by more than 30 states.

The Act imposes substantial new compliance obligations on covered entities, with limited exemptions for certain licensees already subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act. At its core, the law requires each licensee to develop and maintain a written information security programme tailored to the organisation's size, complexity, use of third-party

service providers, and the sensitivity of the non-public information it handles. The law imposes a four-business-day notification requirement for cybersecurity incidents that meet a certain threshold (such as when an event involves 250 or more Missouri consumers' non-public information), which is notably more compressed than the general breach notification standard in Section 407.1500. For insurers and producers that had not previously been subject to a sector-specific data security mandate at the state level, the Act represents a meaningful shift in the compliance landscape.

Legislative Updates

The Missouri legislature has declined to advance any recent bills proposing to enact a comprehensive consumer privacy act. However, the Missouri legislature is currently considering Senate Bill No 1359, which proposes a Biometric Information Privacy Act (BIPA). Unlike Illinois' BIPA, which is consent-centric and enforced through a private right of action, Missouri's BIPA would limit liability by creating a safe harbour for businesses using biometric identifiers, so long as those businesses meet certain compliance standards for consumer notice, retention policies and data security.

The Missouri legislature is also reviewing a proposed Artificial Intelligence Transparency and Accountability Act (SB 1324), which would require labelling of AI-generated content and consent for using a real person's likeness. SB 1324 would authorise enforcement by the Attorney General and by private plaintiffs.

The state house is reviewing House Bill No 3393, which would prohibit social media platforms from allowing persons under 16 years of age to create or maintain accounts separate from a parent or guardian, while minors aged 16 or 17 could hold accounts only with verified parental consent. The bill would also target "addictive or manipulative platform design" by prohibiting features such as infinite-scroll mechanisms and auto-playing content without time-limit controls. The bill would also create a private right of action for parents or legal guardians of harmed minors.

Conclusion

Missouri's privacy enforcement landscape is defined by the creative and aggressive application of the

MMPA rather than by a purpose-built privacy statute. The Attorney General's office has demonstrated a willingness to reach data collection, use and sharing practices through the MMPA's broad prohibition on unfair and deceptive conduct. While the courts have yet to fully test those theories, the enforcement record alone carries compliance weight. Companies operating in or serving Missouri consumers would be well advised to audit their data practices with the pixel litigation in mind, scrutinise privacy disclosures for accuracy against actual data use, and account for the sector-specific obligations layered beneath the MMPA – particularly where health data, financial information or minors are involved.

The absence of a comprehensive privacy law in Missouri should not be mistaken for the absence of meaningful privacy risk. To the contrary, the current patchwork of statutes and regulations heightens operational risk and requires diligent, ongoing compliance review.

USA – NEW YORK



Trends and Developments

Contributed by:

Alan Behr

Phillips Nizer LLP

Phillips Nizer LLP is a full-service law firm celebrating its 100th anniversary. It is widely recognised as one of the signature and historic legal practices in the United States. From offices in New York City and northern New Jersey, the firm practises nationally and assists clients worldwide through a trusted network of international associates. Its three-lawyer data protection and privacy practice is integrated within

the firm's broader intellectual property and technology services practices, advising a distinguished roster of clients in fashion, technology and the arts. Drawing on the firm's depth in intellectual property and commercial law, Phillips Nizer provides practical, business-focused guidance to help clients navigate evolving data and technology issues worldwide.

Author



Alan Behr is a senior partner at Phillips Nizer LLP who concentrates his practice on intellectual property, technology, fashion and the arts. He has long served as a leader within the International Trademark Association,

working in a variety of prominent committee roles that reflect his prominence in the global trade mark community. A widely recognised thought leader, Alan has written and spoken extensively on trade mark, copyright and business relationship issues, and has edited or contributed to six scholarly books on intellectual property law and related topics. He is also a fine-art photographer, with images in the permanent collections of four major museums as well as in corporate and private collections.

Phillips Nizer LLP

485 Lexington Avenue, 14th Floor
New York, New York 10017
USA

Tel: +1 212 841 0552
Fax: +1 212 262 5152
Email: abehr@phillipsnizer.com
Web: www.phillipsnizer.com

PHILLIPS NIZER LLP



Time Exposure: the Evolution of Privacy in New York Photography Cases

The United States of America is unique in its approach to privacy in key ways. Because of its federal system, whatever elements of the law are not expressly made national by the Constitution or by constitutionally permitted federal pre-emption will remain the subject solely of the states and territories. The second component is cultural – a question that itself can be divided for convenience into two parts: the first is the American passion for individual liberty, something that again is embedded in the Constitution and, indeed, in the very Declaration of Independence (1776) by which the nascent country sought to define itself as an autonomous nation; the other leg of that cultural background is, sometimes paradoxically, the American embrace of consumerism. Just as the libertarian ideals of the foundation of the American republic work to guard against governmental authorities knowing too much about the citizenry, the citizens will voluntarily give away personally identifiable information to a high degree in exchange for desired commercial goods and services.

The American approach to privacy therefore requires an understanding of:

- who is asking for it;
- what might be in it for the person making the disclosure, to agree to hand it over; and
- did someone or could someone make money from what happened?

Unlike many legal systems that recognise privacy as a general personal right, in the United States the domain of privacy law is uniquely fragmented, with privacy protections mainly developed by the states, often with statutes drawn for restricted purposes and under narrowly decided case precedent. That becomes particularly apparent when reviewing the rights and responsibilities of parties seeking to publish, display and commercially exploit images bearing presentations of individuals. Rather than granting the subjects of photographs broad control over how their images are captured or disseminated, state laws are typically crafted to protect privacy in clearly defined circumstances – most notably, in recent years, in the collec-

tion and use of information provided by the users of online facilities.

If a core concept had to be gleaned from this, it is the overriding notion (or the “umbrella concept”) as to whether the person in a photograph who claims an invasion of privacy had, in the moment of the asserted intrusion, a “reasonable expectation of privacy”. That is, would the individual fairly believe that a setting sufficiently sequestered a person from the eyes and ears of others as to take comfort that whatever happened in that setting would not be perceived and transmitted, published or displayed? If a man should move through the living room of his home, for instance, would he have a reasonable expectation that a neighbour would not have recorded that with a telephoto lens on a camera aimed through the window of the building opposite? If he should be photographed walking through a public square, would he have a case against the display of a print in the name of fine art? More on both of those examples follows below.

New York State was the first jurisdiction to initiate what could be called the contemporary law of privacy. There was a renowned intellectual predicate, as happens every once in a while in American law. It appeared in an 1890 article by Samuel D Warren and Louis D Brandeis (the future associate justice of the United States Supreme Court) entitled “The Right to Privacy”. The timing was fortuitous, with the article being published shortly after the Kodak company launched the first true consumer camera (from New York State, in fact) with the famous marketing slogan “You Press the Button, We Do the Rest”, and six years before *The New York Times* published its first photograph. It was also the period of “yellow journalism” – scandal-mongering prose published by journalists to boost circulation, all too often at the expense of reputations and even the truth. The authors described privacy as a protection of the “inviolable personality” and famously framed it as the “right to be let alone”. Their conception of privacy emphasised emotional well-being rather than redress for economic damage. They argued that existing legal doctrines, such as property and contract law (both being grounded in commercial law, of course), were inadequate to address the potential personal harms caused by the publication of personal images and information.

Roberson v Rochester Folding Box Co

The origins of the approach of New York State to privacy can be traced to a case decided a mere dozen years after the publication of that article. In *Roberson v Rochester Folding Box Co*, the New York Court of Appeals (the highest court in the state) refused – following a lengthy analysis – to recognise a common-law right to privacy. The plaintiff was a young woman; a photographic portrait of her was used on the box for Franklin Mills Flour and in an advertisement for the product, along with the slogan “Flour of the Family”. The plaintiff claimed that the use of her likeness to sell goods caused her humiliation and distress. The court expressed concern that recognising such a right would lead to “limitless liability, and that the adoption of such a right would result in a vast amount of litigation, that would border upon the absurd”.

The decision in *Roberson* proved controversial, and was an impetus for the passage by the New York State Legislature during the following year of the first law in the United States enacted to prevent the unauthorised use of an individual’s name or image for commercial purposes. The legislation remains on the books as Civil Rights Law Sections 50 and 51, which jointly created a statutory right of privacy that prohibits the unauthorised commercial use of a person’s name or likeness under certain conditions. It remains at the core of all privacy inquiries in New York State, with there still being no common-law right of privacy recognised by the courts.

Murray v New York Magazine Co

The most important question, perhaps, is how this might affect the use of photographs in reporting the news, which enjoys strong protections under the First Amendment to the Constitution. The news photography case of *Murray v New York Magazine Co* went to the state’s highest court on the basis of a complaint pursuant to Section 51 of the Civil Rights Law. The plaintiff was a man who was not of Irish descent but who liked to dress so characteristically Irish (to witness the New York City St Patrick’s Day parade) that a photograph taken of him without his knowledge was used one year later on a magazine cover to illustrate an article in the New York Magazine entitled “The Last of the Irish Immigrants”, by no less a journalistic talent than the inimitable Jimmy Breslin. The plaintiff had to

concede that the Breslin piece concerned an event of public interest that his photograph was used to illustrate, and the court granted summary judgment to the defendant.

Arrington v New York Times Co

In *Arrington v New York Times Co* (1982), the plaintiff claimed that his image was made the most prominent illustration in an article published in *The New York Times Magazine* entitled “The Black Middle Class: Making it”. He sued under the Civil Rights Act, notably because he objected to being cast as an “exemplar” of a social class and because he did not agree with ideas expressed in the story. The Court of Appeals held that New York courts should not avoid parsing through views on social issues in deciding privacy cases under the Civil Rights Law. Putting that question aside, therefore, it easily applied the “newsworthiness exception” of the *Murray* case to rule in favour of the defendant.

Finger v Omni Public Intl

The case of *Finger v Omni Public Intl* (1990) concerned a photograph of Joseph and Ida Finger and their six children, which had been used to illustrate an article in the magazine *Omni* on the claimed benefits of caffeine in the demanding and still quite uncertain process of conception by in vitro fertilisation. Even though none of the six Finger children had been the result of in vitro fertilisation (caffeinated or otherwise), again due to the newsworthiness of the piece the court affirmed dismissal of the complaint.

Messenger v Gruner + Jahr Printing and Publishing

In 2000, the Court of Appeals helpfully summarised and synthesised its holdings in *Murray*, *Arrington* and *Finger*. The case was *Messenger v Gruner + Jahr Printing and Publishing*. In *Messenger*, the plaintiff suing under the Civil Rights Law was a 14-year-old aspiring model who posed for a series of magazine photographs. Only later did the model discover that her photograph had been used in the magazine *Young and Modern* to illustrate an article entitled “Love Crisis”, which began with a letter to the editor by a different 14-year-old who reported getting drunk at a party and then having sex with her 18-year-old boyfriend and two of his boon companions.

The court articulated a clear rule:

“Consistent with the statutory – and constitutional – value of uninhibited discussion of newsworthy topics, we have time and gain held that, where a plaintiff’s picture is used to illustrate an article on a matter of public interest, there can be no liability under Sections 50 and 51 until the picture has no real relationship to the article or the article is advertisement in disguise.”

In simple terms, there is a three-part test applicable to news media. There is no actionable claim under the Civil Rights Act if:

- the photograph illustrated that an article has newsworthiness (which, the court made clear, “is to be broadly construed”);
- there was a real relationship between the image and the story; and
- the writing was not “advertising in disguise” (such as presumably would be advertorial).

A high bar has thereby been set when seeking to assert a claim of privacy against a photograph used as news; however, what if the use is not merely advertising in disguise but advertising presented as such?

Cohen v Herbal Concepts Inc

In 1984, the New York Court of Appeals decided *Cohen v Herbal Concepts Inc* (1984). The facts relied upon by the court in its decision were simple: a young mother, Susan Cohen, and her small daughter were surreptitiously photographed from behind, their faces not visible, while wading nude in a stream on private property. Without consent, the image was later used in an advertisement by Herbal Concepts for a preparation designed to fight cellulite – the commercial message being that the condition clearly did not trouble the woman in the image. Ms Cohen, along with her husband, filed an action under New York Civil Rights Law Section 51, claiming that privacy had been violated through the unauthorised commercial use of their image. The Court ruled that a person can be considered identifiable even if her face is not shown in a photograph. Identifying features could include “their hair, bone structure, body contours and stature and their posture”. Identification of Ms Cohen and her daughter from those features such that a violation of

the Civil Rights Act would follow was a matter for the jury to determine, and so the court allowed the privacy claim to proceed.

However, what if there is no news and the use is not in advertising, but a question arises as to *ars gratia artis* (art for art’s sake)? Art about which the public is aware is nearly always made for display and sale in the art marketplace; does that make an art photograph something in “trade” under the Civil Rights Act?

Nussenzweig v diCorcia

In *Nussenzweig v diCorcia* (2007), the Court of Appeals dismissed a privacy claim arising from candid photographs taken in Times Square and later exhibited in an art gallery. Philip-Lorca diCorcia did what photographers have been doing in earnest on New York City streets since the launch of the first Leica camera over a century ago: snapping images of passersby. While in Times Square, he made multiple images, one of which turned out to be of Erno Nussenzweig, who was caught wearing traditional Hasidic Jewish attire and was shown with his bearded face in view. That photograph became one of 17 by diCorcia displayed in a fine art exhibition at Pace/MacGill Gallery entitled *Heads*. The defendants won on summary judgment because the claim had been time-barred by the one-year statute of limitations that applies to Civil Rights Act claims. It is useful just the same to examine the concurring opinion from the lower appellate court. It reached into the question of the application of the First Amendment, opining that “inclusion of the photograph in a catalog sold in connection with the exhibition of the artist’s work did not render its use commercial pursuant to the privacy statute”, with the expression of the artistic ideas behind the work being protected by the First Amendment.

Foster v Svenson

Similarly, in *Foster v Svenson*, the Appellate Division of the New York County Supreme Court First Department decided that candid art photographs – this time of people in private spaces – fell outside the Civil Rights Act. The defendant, the fine-art photographer Arne Svenson, took candid telephoto pictures through the window of his apartment in a neighbouring building, capturing residents visible to him through the largely glass façade of the building opposite. Included in his

oeuvre were identifiable images of the Foster family, including young children. These images were then assembled into a series titled *The Neighbors*, exhibited and sold in galleries in Los Angeles and New York City; some were later shown in media coverage about the exhibitions. The people in the photographs may have had no idea they were being observed, let alone photographed, through their windows – but this time art won, with dismissal of the complaint on motion by the defendant.

Other Key Considerations

There can be other considerations under New York law as well as the Civil Rights Act. In *Perry v Rockmore* (2025), the appearance on commercial websites of before-and-after photographs of the plaintiff's rhinoplasty surgery did not support a claim under Sections 50 and 51 of the Civil Rights Act but did give rise to liability for breach of the fiduciary duty of doctor-patient confidentiality.

Other doctrines of law might also have their say from time to time. In a way that has gone in and out of the national legal system with iterating perplexity, privacy slipped into constitutional law and now kind of rattles around inside it. In 1965, in the case of *Griswold v Connecticut*, the Supreme Court found a right of marital privacy in the “penumbras” of the Constitution, requiring protection from state attempts to restrict contraception. That reasoning was applied again by the Supreme Court in *Roe v Wade*, which recognised a constitutional right to abortion. *Roe* was partially reaffirmed in *Planned Parenthood v Casey*, but both cases were overruled by *Dobbs v Jackson Women's Health Organization*. *Roe* was expressly overruled as to whether having an abortion is a right protected by the Constitution. The constitutional right of privacy recognised in *Griswold* and *Roe* remains formally (however nominally) intact.

It would be remiss not to close this section with a (so far) indirectly related turn in New York law: in 1992, the Court of Appeals ruled in *People v Santorelli* that, as men had been permitted by law since 1937 to be seen shirtless in public, with the limited exception of actions taken in furtherance of commercial purposes, it is perfectly lawful for any New York woman to go about in public naked from the waist up. Custom and usage continue to make that a right largely without practitioners, but it hints at an open-minded approach to what does or does not constitute a state of personal display to which an expectation of privacy attaches within New York State.

Where does that leave us in New York? Virtually everyone now has with them a phone camera capable of taking photographs that can be posted internationally within seconds following completion. If you want to start a (potentially expensive) lawsuit about whatever happens with that, it would be wise to consider whether you have truly good reason to move forward and if less confrontational options for making your feelings known might be available.

USA – TENNESSEE



Trends and Developments

Contributed by:

Alisa Chestler, Matthew White and Andrew Droke
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Baker, Donelson, Bearman, Caldwell & Berkowitz, PC and its data protection, privacy and cybersecurity team advises clients across the full life cycle of information management, from privacy and data security planning and program design to regulatory compliance and data breach response. The team is recognised as an Authorized Breach Coach by NetDiligence and regularly assists organisations navigating complex cybersecurity incidents, regulatory inquiries and enforcement actions. The team has deep experience in advising on a wide range of federal, state and international privacy and data security laws, includ-

ing the CCPA, CPRA, CIPA, GDPR, HIPAA, GLBA, TCPA, COPPA, FCRA and related statutes. Beyond compliance counselling, the team routinely represents clients in high stakes litigation and investigations arising from data breaches and cyber-incidents. Representative matters include defending national and global companies in class action litigation following phishing attacks and large scale data incidents, responding to alleged FTC guideline violations, and serving as incident response leads and law enforcement liaisons for clients across multiple industries.

Authors



Alisa Chestler (CIPP/US, QTE) serves as the chair of Baker Donelson's data protection, privacy and cybersecurity team. She concentrates her practice on privacy, security, artificial intelligence (AI) and information

management issues, including compliance, contract negotiation and corporate transactions matters. She joined Baker Donelson after a distinguished career as in-house counsel and privacy officer for several large public and private companies, including several managed care organisations and healthcare companies. Alisa is a Certified Information Privacy Professional – United States (CIPP/US) and has also attained certification as a Qualified Technology Expert (QTE).



Matthew White (AIGP, CIPP/US, CIPP/E, CIPT, CIPM, PCIP) is co-chair of Baker Donelson's financial services cybersecurity and data privacy team, and is a member of the firm's incident response team, which has been

named an Authorized Breach Coach by NetDiligence. He regularly advises clients on matters related to cybersecurity, data privacy, technology and artificial intelligence (AI). Matthew focuses on counselling his clients on a wide range of issues including compliance, policies and procedures, training, transactions, contracts, incident response, regulatory investigations, litigation and arbitration.



Andrew Droke (CIPP/US) leads Baker Donelson's artificial intelligence (AI) and General Data Protection Regulation (GDPR) teams, and counsels clients in a broad range of data protection, privacy and cybersecurity matters. As a member of the firm's health law group and data protection, privacy and cybersecurity team, Andrew advises clients regarding complex data use and sharing arrangements, digital health strategies, technology agreements, and information privacy and security compliance considerations.

Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

1600 West End Avenue
Suite 2000
Nashville, TN 37203
USA

Tel: +1 615 726 5600
Fax: +1 615 726 0464
Web: www.bakerdonelson.com

BAKER DONELSON

Tennessee's reputation as a business-friendly state is well earned; however, when it comes to data protection, the regulatory landscape has evolved rapidly. Over the last few years, the state has enacted several new laws governing how businesses collect, use and safeguard personal data, as well as how they deploy emerging technologies such as artificial intelligence (AI). From the Tennessee Information Protection Act to first-of-its-kind AI legislation, these laws carry real operational implications across industries, and the consequences of non-compliance are significant. This guide provides a practical overview of the key Tennessee requirements with respect to privacy, data security and technology, equipping businesses with the foundation they need to navigate this shifting terrain.

Privacy

Tennessee has adopted a comprehensive consumer privacy law as well as industry-specific privacy requirements, creating a state-specific patchwork of obligations. Businesses in Tennessee must understand both the generally applicable laws as well as those that apply specifically to their industry.

The Tennessee Information Protection Act

Like many other states, Tennessee has adopted a comprehensive consumer privacy law. The Tennessee Information Protection Act (TIPA) went into effect on 1 July 2025, and certain aspects are similar to comprehensive privacy laws enacted in other states. However, as discussed in more detail below, many of TIPA's requirements are unique, and businesses should carefully assess compliance.

Applicability

TIPA applies to persons who meet the following criteria:

- either conduct business in Tennessee or produce products or services that are targeted to residents of Tennessee; and
- have more than USD25 million in annual revenue; and
- either control or process the personal information of at least 175,000 Tennessee consumers during a calendar year, or control or process the personal information of at least 25,000 Tennessee consumers and derive 50% of their gross annual revenue from the sale of that information.

Although these thresholds mean that many small businesses in Tennessee will not be subject to the law, it is important for businesses to regularly monitor both their revenue and their data-related activities to assess whether the law applies.

In addition to tailoring its scope via the thresholds discussed above, TIPA also limits its applicability with several exceptions. By way of example, TIPA does not apply to:

- governmental agencies;
- non-profit organisations;
- covered entities and business associates subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- higher educational institutions (public or private);
- insurance companies licensed under state law; and

- financial institutions and their affiliates subject to the Gramm-Leach-Bliley Act (GLBA).

However, as is the case in all jurisdictions, the entity-level exemptions under TIPA should be reviewed carefully.

Personal information

TIPA defines “personal information” broadly as “information that is linked or reasonably linkable to an identified or identifiable natural person”. However, the law narrows this scope through several data-level exemptions. For example, TIPA does not apply to:

- health records under state law and protected health information under HIPAA;
- personal information processed for research purposes under applicable law;
- consumer credit reporting data;
- personal or educational information regulated by the Family Educational Rights and Privacy Act (FERPA);
- personal information collected, processed, sold or disclosed under the federal Farm Credit Act;
- employment-related data processed in the course of an individual’s application, employment or work as an agent or independent contractor;
- publicly available information;
- de-identified data created under HIPAA;
- de-identified data as defined under TIPA, provided that certain requirements are met; and
- aggregate consumer information.

Given these exemptions, organisations should carefully identify the data they process and determine whether any exemptions apply.

It is also important to assess whether any personal information being processed is considered “sensitive data”. Under TIPA, “sensitive data” includes the following:

- personal information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
- genetic or biometric data processed to uniquely identify a natural person;

- personal information collected from a known child; and
- precise geolocation data.

Sensitive data may only be processed with the consumer’s consent (ie, a clear affirmative act signifying a consumer’s freely given, specific, informed and unambiguous agreement), and any sensitive data concerning a known child must be processed in accordance with the Children’s Online Privacy Protection Act (COPPA).

Basic responsibilities of controllers and processors

Like other US state privacy laws and the EU’s General Data Protection Regulation (GDPR), TIPA assigns responsibilities to parties based on their roles, using the common terminology of “controllers” (ie, those determining the purpose and means of processing personal information) and/or “processors” (ie, those who process the personal information on the controller’s behalf). This is a fact-based determination that depends on the context in which the personal information is being processed.

Under TIPA, controllers must meet the following requirements.

- Data minimisation: controllers must limit their collection of personal information to what is adequate, relevant and reasonably necessary for the disclosed processing purpose.
- Privacy notice: controllers must provide a clear, reasonably accessible privacy notice disclosing the categories and purposes of data processed, how consumers may exercise their rights, and information about any sales or personal information or targeted advertising activity, including how to opt out.
- Secondary use prohibition: controllers may not process personal information beyond the purposes disclosed to the consumer without first obtaining the consumer’s consent.
- Data security: controllers must implement reasonable administrative, technical and physical safeguards appropriate to the volume and nature of the personal information they process.
- Non-discrimination: controllers must not process personal information in a manner that violates

anti-discrimination laws and may not discriminate against consumers who exercise their rights under TIPA.

- Data protection assessments – controllers must conduct and document data protection assessments, which may be requested by the Tennessee Attorney General, regarding the following processing activities:
 - (a) processing personal information for purposes of targeted advertising;
 - (b) sales of personal information;
 - (c) processing personal information for the purpose of profiling in certain situations;
 - (d) processing of sensitive data; and
 - (e) processing activities that present a heightened risk of harm to consumers.
- Data processing agreements: controllers must enter into a binding contract with each processor that processes personal information on their behalf. The agreement must instruct the processor about the processing of data and describe the nature, purpose, type of data and duration of processing, as well as the rights and obligations of both parties. The agreement must also require the processor to:
 - (a) impose confidentiality obligations on those involved in the processing;
 - (b) delete or return personal information at the controller's request at the end of the provision of services;
 - (c) make compliance-related information available to the controller;
 - (d) co-operate with assessments; and
 - (e) flow down equivalent requirements to any subcontractors.

Beyond their contractual duties, TIPA also imposes direct obligations on processors, requiring them to:

- adhere to the controller's instructions;
- enter into binding data processing agreements; and
- assist the controller with its obligations under TIPA, including by adopting appropriate measures to help respond to consumer requests and providing information necessary for data protection assessments.

Consumer rights

Similar to the privacy laws enacted in other states, TIPA affords Tennessee consumers the following rights with respect to their personal information:

- the right to confirm whether a controller is processing the consumer's personal information;
- the right to access their personal information;
- the right to correct inaccuracies in their personal information;
- the right to delete their personal information;
- the right to obtain a portable copy of the personal information that the consumer previously provided to the controller; and
- the right to opt out of the sale of personal information about them, targeted advertising, and profiling in furtherance of decisions that produce legal or significant effects.

Controllers must respond to consumer requests without undue delay, and, in all cases, within 45 days of receiving the request. Similar to other states, Tennessee has also implemented authentication requirements, a framework under which the controller can extend the timeline for responding, and an appeals process that can be utilised by the consumer.

Enforcement and unique affirmative defence

TIPA is enforced exclusively by the Tennessee Attorney General, and there is no private right of action. The law also specifically prohibits violations of TIPA from serving as the basis for private claims or class action lawsuits. Controllers and processors found in violation may face civil penalties of up to USD7,500 per violation, and courts may impose treble damages for knowing or wilful violations.

One of TIPA's most distinctive features is its affirmative defence provision. A controller or processor that adopts and maintains a privacy programme that "reasonably conforms" to the National Institute of Standards and Technology (NIST) Privacy Framework, or similar documented policies, standards and procedures designed to safeguard consumer privacy, can establish an affirmative defence against enforcement actions. The programme must also provide individuals with the rights afforded under TIPA and be regularly updated and appropriately tailored to the organisa-

tion. This creates a meaningful incentive for businesses to invest in robust privacy programmes – not only to improve their operations but to build a concrete legal safeguard against potential enforcement.

Tennessee's Genetic Information Privacy Act

In addition to TIPA, Tennessee has also adopted the Genetic Information Privacy Act (GIPA). GIPA regulates direct-to-consumer genetic testing companies and requires them to provide consumers with information about the collection, use and disclosure of their genetic data as well as a publicly available privacy notice covering the company's data collection, consent, use, access, disclosure, transfer, security, retention and deletion practices. Companies must obtain the individual's express consent for collecting, using and disclosing genetic data, and other uses and disclosures – such as disclosures to an individual's employer – require separate consents.

In addition to the notice and consent requirements, genetic testing companies must also:

- develop, implement and maintain a comprehensive security programme;
- support processes that allow consumers to access their genetic data, delete their account and genetic data, and destroy biological samples; and
- only disclose genetic data to law enforcement or government entities in response to valid legal process if the consumer has not provided express written consent.

This law is enforced by the Tennessee Attorney General.

Data Security

Beyond the data security obligations imposed by TIPA, Tennessee has adopted several other laws that establish data security and breach notification requirements for businesses.

Breach notification

Tennessee's breach notification law applies broadly to any person or business that conducts business in the state and owns or licenses computerised personal information of Tennessee residents. Under the law, an "information holder" must notify affected individu-

als within 45 days of discovering or being notified of a breach of "system security", which is defined as the unauthorised acquisition of data that materially compromises the security, confidentiality or integrity of personal information. Importantly, the law does not apply to entities subject to the GLBA or HIPAA, and it includes a "materially compromises" threshold that effectively limits the notification obligation to breaches that pose a meaningful risk of harm to affected individuals.

Notably, unlike TIPA, the breach notification law provides a private right of action, and injured individuals may bring civil claims for damages and injunctive relief. However, Tennessee enacted a significant class action shield in 2024 providing that a private entity is not liable in a class action lawsuit resulting from a cybersecurity event unless the event was caused by wilful and wanton misconduct or gross negligence. This heightened standard substantially limits class action exposure for businesses that experience a data breach but have otherwise maintained reasonable cybersecurity practices. This protection is particularly significant given the nationwide surge in data breach class action filings in recent years, and it goes further than the approach taken in other states, such as Ohio and Connecticut, which offer only affirmative defences to entities that maintain conforming cybersecurity programmes, rather than a broad class action shield tied to the defendant's level of culpability. Notably, courts have held that this provision does not apply retroactively to cybersecurity events that occurred before its effective date.

The Insurance Data Security Law

Tennessee has also adopted an Insurance Data Security Law, which requires licensed insurers to develop, implement and maintain a comprehensive information security programme. Licensees must investigate cybersecurity events and notify the Commissioner of Commerce and Insurance as well as affected consumers within 45 days of determining that a cybersecurity event has occurred. This law includes exceptions for smaller licensees (eg, those with fewer than 25 employees or less than USD5 million in gross annual revenue).

Record disposal and Social Security number protections

Finally, Tennessee imposes additional data security obligations through its identity theft statutes. Businesses must take reasonable steps to destroy personal identifying information contained in customer records before disposal, with violations punishable by civil penalties of up to USD500 per record (capped at USD10,000 per customer). Separately, businesses that obtain Social Security numbers must make reasonable efforts to protect them from public disclosure, including prohibitions on transmitting them over unsecured internet connections and printing them on mailed materials.

Taken together, these laws create a layered set of data security obligations for businesses operating in Tennessee. While the class action shield provides meaningful protection, businesses should not treat it as a substitute for robust cybersecurity practices. Proactive investment in cybersecurity infrastructure and incident response planning remains the most effective strategy for minimising both legal exposure and operational risk.

Technologies

Finally, in addition to the privacy and security laws discussed above, Tennessee has adopted various laws focused on specific technologies that also impact how businesses in Tennessee consider their data protection obligations and strategies.

The Protect Tennessee Minors Act

In 2024, following several other states, Tennessee enacted the Protect Tennessee Minors Act, which is an age verification law aimed at shielding minors from accessing explicit material online. The law applies to any person or commercial entity that publishes or distributes in Tennessee a website where 33.33% or more of the content is “harmful to minors”. “Harmful to minors” is defined as including nudity, certain sexual content, excess violence or sadomasochistic abuse that:

- would appeal predominantly to the prurient, shameful or morbid interests of minors;

- is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and
- lacks serious literary, artistic, political or scientific values for minors.

The law requires covered entities to verify users’ ages using a “reasonable age-verification method” that cannot be easily bypassed and either matches a live photograph to a valid government-issued ID or uses a commercially reasonable method relying on transactional data to confirm that the user is at least 18 years of age.

Entities performing age verification must retain at least seven years of anonymised verification data but may not retain any personally identifying information after access is granted.

Failing to implement the required age verification is a Class C felony, and the Tennessee Attorney General may bring enforcement actions against non-compliant entities.

The Protecting Children from Social Media Act

Tennessee has also adopted the Protecting Children from Social Media Act, which requires websites and applications that allow users to create accounts and communicate with others to verify users’ ages. If a user is under 18 years old, the platform must obtain express parental consent before allowing the minor to create an account, and must provide parents with tools to supervise the account including privacy settings, daily time restrictions and scheduled breaks. The law is enforced by the Tennessee Attorney General, with civil penalties of up to USD1,000 per violation.

AI legislation

Tennessee has not yet adopted a comprehensive AI law. Instead, the state’s legislative efforts have focused on niche areas.

By way of example, in 2024, Tennessee adopted a first-of-its-kind law addressing the use of AI. The Ensuring Likeness Voice and Image Security (ELVIS) Act amended Tennessee’s existing right of publicity statute to include protections for individuals’ voices from the misuse of AI, expanding upon the protec-

tions already given to name, photograph and likeness. The term “voice” includes “a sound in a medium that is readily identifiable and attributable to a particular individual, regardless of whether the sound contains the actual voice or a simulation of the voice of the individual”. As a result of the updates, the unauthorised use of an individual’s name, photograph, voice or likeness gives rise to a civil claim, and the violation is also a Class A misdemeanour.

The ELVIS Act also established a cause of action that can be asserted against providers of AI tools whose “primary purpose or function” is producing an individual’s photograph, voice or likeness without proper authorisation. This provision may subject certain AI technology providers to a new form of liability, although the “primary purpose or function” requirement remains somewhat ambiguous.

Tennessee also adopted education-specific requirements related to AI in 2024, requiring all state universities, local education agencies, and public charter schools to adopt policies regarding the use of AI by students, teachers and staff. Additionally, in 2025, the state required the Department of Education to develop guidance on social media and internet safety, including the importance of evaluating AI-generated information and understanding the potential for misinformation.

Finally, while the state’s current AI-related legislation is relatively narrow in scope, the Tennessee legislature appears poised to enact further AI-related legislation. The legislature is currently considering bills that would:

- prohibit AI systems from being advertised as qualified mental health professionals;
- criminalise training AI to, among other items, encourage suicide or homicide, act as a licensed health professional, or develop emotional relationships with individuals; and
- require disclaimers in political advertising containing AI-generated content and deepfakes.

It is unclear which, if any, of these bills will become law, but businesses must be mindful of the new and emerging requirements applicable to AI in Tennessee.

Conclusion

Tennessee’s privacy and data protection landscape has expanded significantly in recent years, and the pace of change shows no signs of slowing. From TIPA’s comprehensive consumer privacy framework to the state’s first-of-its-kind AI legislation, businesses operating in Tennessee must navigate a growing web of obligations that touch nearly every aspect of how they collect, use and safeguard personal data.

While this guide has addressed the state’s generally applicable privacy, data security and technology laws, businesses should also be mindful that additional requirements may apply depending on their industry. For example, entities in the healthcare, financial services, insurance and education sectors may be subject to overlapping federal and state requirements that impose additional or more specific data protection obligations. Given the breadth and evolving nature of these requirements, businesses should regularly assess their compliance posture, invest in robust privacy and security programmes, and monitor legislative developments to stay ahead of new obligations as they arise.

USA – TEXAS



Trends and Developments

Contributed by:

Christina Morgan, Jason Blackstone and Matthew Yarbrough
Buchalter LLP

Buchalter LLP is a full-service law firm with over 560 attorneys across 35 practice areas. The Privacy and Data Security team helps clients navigate local, state, federal, and international privacy and data security laws, including multi-state and multi-national compliance and industry-specific self-regulatory frameworks. The firm advises across industries on website practices, data collection and storage, privacy programme development, breach notification obligations, and responses to investigations, penalties, and related litigation. Interdisciplinary by design, Buchal-

ter draws lawyers from litigation, healthcare, intellectual property, finance, corporate, and employment to integrate privacy compliance and cybersecurity into business operations and keep decisions practical and defensible. Buchalter is adept at dealing directly with key policy and technical principles to provide policies, procedures, and technical implementations that can be easily operationalised while remaining flexible to endure in the face of ever-changing regulations and threat actors.

Authors



Christina Morgan is a Certified Information Privacy Professional and co-chair of the Privacy and Data Security practice group at Buchalter LLP. She is well versed in consumer privacy laws, including the California

Consumer Privacy Act (CCPA) and the Texas Data Privacy and Security Act (TDPSA). Ms Morgan routinely conducts privacy reviews and counsels clients on privacy compliance and consent management. She has prepared myriad policies and terms for client websites, including privacy policies, notices of collection, and terms of service. Ms Morgan also supports clients who are sharing personal information with vendors and other third parties by negotiating data processing agreements.



Jason Blackstone is an experienced intellectual property litigator who has focused on bringing an interdisciplinary, asset-based view of cybersecurity and data privacy practice. He has guided clients in

both reactive scenarios dealing with breaches and unconventional threats and on the proactive side,

preparing clients for argument before fact finders through an emphasis on the singular story approach. He has dealt extensively with artificial intelligence for over a decade and successfully counselled clients on data life cycle, data governance, cybersecurity, data asset management, and created evergreen, reactive privacy and data management systems.



Matthew Yarbrough is an internationally recognised trial lawyer, former federal prosecutor, co-creator of the Texas AG's Internet Bureau, and the FBI's Texas Computer Forensics Laboratory. He has over 30

years of experience in IP, cybersecurity and data privacy. He has conducted more than 2,000 internal corporate investigations involving governance, compliance, securities fraud, cybersecurity, and trade secret theft. As an Assistant U.S. Attorney, Matthew prosecuted high-profile cybersecurity cases: U.S. v. Gl0balHell; and U.S. v. PhoneMasters. He led the DOJ's first-of-its-kind trial task force, Criminal Intellectual Property and Computer Crimes. He has also authored numerous articles, including "Suing the Insecure in Cyberspace."

Buchalter LLP

2626 Cole Avenue
Suite 300
Dallas
Texas 75204
USA

Tel: +1 (214) 263 7500
Email: myarbrough@buchalter.com
Web: www.buchalter.com

Buchalter

Texas Enacts the Texas Data Privacy and Security Act, Adding to the Patchwork of US Consumer Privacy Laws

The Texas Data Privacy and Security Act went into effect on 1 July 2024. As a result, Texas joined a growing number of states that have enacted comprehensive consumer privacy laws. Similar to other states, the TDPSA gives consumers rights to:

- confirm whether a business is processing the consumer's personal data;
- access the personal data collected by the business in a portable and, to the extent feasible, readily useable format that allows the consumer to transmit personal data to another controller without hindrance;
- correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;
- delete personal data provided by or obtained about the consumer; and
- opt out of the processing of the personal data for purposes of: (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

Businesses must honour those rights and cannot discriminate against consumers who choose to exercise their rights. Businesses must also disclose certain information in a privacy policy.

Unlike the California Consumer Privacy Act of 2018, the TDPSA does not create a private right of action. Any violations are enforced by the Attorney General.

Texas Adopts New Law to Promote Children's Privacy

Texas is one of several states that have enacted laws that impose requirements on app stores and app developers related to the use of mobile apps by minors. The Texas App Store Accountability Act would require app stores to verify user ages at the time of account creation and to obtain parental consent before minors can download apps or make in-app purchases. The Act would help prevent inadvertent privacy violations caused by inaccurate self-reporting. For instance, a child would be unable to put in a fake age to download an app not intended for minors.

Texas's law was scheduled to go into effect on 1 January 2026. However, it is currently subject to litigation in the United States District Court for the Western District of Texas. On 23 December 2025, a federal judge issued preliminary injunctions preventing the law from taking effect.

Uncertain Future for Numerous New Texas AI Laws

Texas has passed a number of new laws relating to the use of artificial intelligence, including:

- HB 441: Act Relating to the Regulation and Use of AI by Governmental Entities, effective 1 September 2025;
- HB 1999: AI Sexual Material Harmful to Minors, effective 1 September 2025;

- HB 149: Financial Abuse Using Artificially Generated Media or Phishing, effective 1 September 2025;
- H 878: Unlawful Production or Distribution of Certain Sexually Explicit Material, effective 1 September 2025;
- SB 1361: Use of Automated Decision System for Adverse Determinations, effective 1 September 2025;
- HB 581: Visual Material Appearing to Depict a Child; and
- Texas Responsible Artificial Intelligence Governance Act, effective 1 January 2026.

These laws are in limbo, however. On 11 December 2025, President Trump issued an executive order, which threatened to pull federal broadband funding from states that enacted “onerous” AI laws. Texas was awarded USD3.3 billion in federal funding to expand broadband access in the state. This has put lawmakers on both sides of the aisle in conflict with the federal government.

Data-Light AI Lets You Compete With Less Personal Information

The legal community and general counsels especially have spent the last decade hearing a single refrain from the business side. More data means better decisions. More data means better personalisation. More data means more growth. Privacy and cybersecurity teams have been the necessary brakes, asking whether the organisation really needs to keep what it collects and whether it can defend those practices when something goes wrong. The inherent balance of when data goes from an asset to a liability has been a battlefield within many organisations, often without a clear answer. That tension is not going away; it is changing form.

AI is accelerating the shift from data as fuel to models as leverage. That shift does not end privacy and cybersecurity risk; it changes what you must govern, what you must document, and what you must be able to explain to regulators, legislators, and fact finders. In a world of AI agents and advanced automation, the most sophisticated organisations will be those that can move quickly with minimal retained personal data, while still proving that their systems are controlled, auditable, and reasonable.

This future does not promise that AI eliminates the need for data, because it does not. It argues that AI changes where data lives, how long it should live there, and what it should be allowed to do. It then offers a flexible approach to privacy and cybersecurity that is designed for unpredictability. Threats evolve faster than policies. Regulations evolve faster than roadmaps. Your governance must be built for change at low cost, without requiring a small army of outside developers to rewrite core controls every time the world shifts.

Texas Biometric Laws Weigh on a Data-Light AI-Driven Approach

AI-driven identity and personalisation strategies often drift toward biometric identifiers because they are convenient for authentication, fraud controls, and user experience. In Texas, the Capture or Use of Biometric Identifier Act (CUBI) creates a direct statutory compliance hook: a person may not capture an individual's biometric identifier for a commercial purpose without first informing the individual and obtaining consent, and the statute restricts disclosure, requires reasonable care in storage and transmission, and imposes a destruction requirement tied to the purpose for which the biometric identifier was collected. The Texas Attorney General highlights these requirements and emphasises that enforcement sits with the AG and may include civil penalties per violation.

For governance design, this matters because “data light” architectures can unintentionally become “biometric heavy” architectures. A defensible programme therefore treats biometric ingestion as a controlled exception with heightened notice, consent, retention limits, and audit logging, rather than as an incidental by-product of modern AI tooling.

The New Premise: You Cannot Forecast the Next Threat, Statute, or Theory of Liability

Most compliance programmes assume the future will look like the past. That assumption is now the liability. Cybersecurity threats mutate weekly. AI systems change behaviour as prompts, plugins, tools, and downstream integrations evolve. Meanwhile, lawmakers are moving toward risk-based AI rules that require impact assessments, disclosures, and documented

mitigation, even when the technology stack is still in flux.

The winning move is not to hard-code today's requirements into brittle systems. The winning move is to build an adaptable governance and technical architecture that lets you change quickly, prove what you did, and explain why it was reasonable. That is the posture that translates across regulators and juries, even when statutes and threats mutate.

The Core Idea: AI Can Reduce the Need to Retain Detailed Personal Data, but It Cannot Eliminate Accountability

Instead of retaining detailed consumer data, create virtual consumer avatars, score interactions, and use that scored experience to test marketing and deliver personalisation while retaining only contact information and regulatory essentials. The strategic objective is clear. Minimise retained personal data while preserving the ability to learn, optimise, and personalise.

This is directionally aligned with data minimisation principles. Regulators, including the FTC, have framed good security and privacy as collecting only what you need, keeping it safe, and disposing of it securely. That is both a compliance theme and a litigation risk theme. The less you retain, the less you lose in a breach and the less you must defend in discovery.

But legal counsel for an organisation should also see the trap. Even if you delete raw event-level consumer data, you may still be “processing” personal data through models, derived profiles, and inferences. Many regimes treat inferences as personal data if they can be linked to a person, even indirectly. AI does not make personal data disappear. It changes its shape. That is why a “data-light” strategy must be paired with governance that addresses profiling, transparency, discrimination risk, and security of the model life cycle.

So the practical answer is to refine the avatar concept into a defensible privacy-enhancing architecture. You can reduce retention while keeping learning and personalisation, but you have to do it in a way that is explainable, auditable, and adaptable.

Privacy and Cybersecurity in a “Model-First” World: What Changes, What Stays

The most important change is that models become regulated assets. The NIST AI Risk Management Framework frames AI risk management as a socio-technical discipline with core functions to govern, map, measure, and manage. It explicitly calls for accountable and transparent systems, explainability, privacy enhancement, and security and resilience. Those are not optional qualities if you want to survive regulatory scrutiny.

The second change is that privacy programmes cannot stop at data inventories and retention schedules. You now need model inventories, training data provenance, documentation of intended use, and monitoring of drift and downstream integrations. The EU AI Act's emphasis on documentation, transparency, and risk categorisation is consistent with this trajectory. In many organisations, the best privacy policy in the world will fail if the model supply chain is a black box.

The third change is that cybersecurity must extend to the AI life cycle. Traditional security focuses on networks, endpoints, and data stores. AI introduces new attack surfaces, including prompt injection, model inversion, data poisoning, and supply chain compromises through third-party components. Even when using privacy-preserving approaches like federated learning, literature recognises that model updates can leak sensitive information without additional protections.

What stays the same is the core legal narrative. Reasonable care. Foreseeability. Good faith controls. Truthful disclosure. If you can show that your organisation collected only what it needed, protected what it kept, disposed of what it did not need, and governed AI decisions with documentation and oversight, you are building a posture that survives both regulators and juries.

Flexibility as a Compliance Strategy, Not a Buzzword

An organisation cannot hard code privacy and cybersecurity into rigid systems because future threats and regulations cannot be predicted. The next wave of enforcement will reward organisations that can adjust

quickly and prove they did so responsibly. The strategy is to design flexibility into both policy and technology.

This approach highlights the need for an AI governance programme that includes safety testing, documentation, and harm mitigation, and points to standards frameworks such as NIST and ISO as part of compliance thinking. That is consistent with what regulators are asking for: not perfection, but a programme.

Flexibility is also about cost and speed. A programme that requires outside contractors to make routine changes is not agile; it is a bottleneck. The operational goal should be to empower internal owners to adjust retention schedules, change model routing rules, update prompts and guardrails, and change vendor integrations without a rebuild. This is governance through configuration, not governance through heroic engineering projects.

Portability and Vendor Independence

Vendor lock-in is not only a procurement problem; it becomes a privacy and cybersecurity problem the moment your vendor's model behaviour changes, your risk tolerance changes, or a regulator asks you to switch approaches quickly. If you cannot move your data, your features, and your model outputs to another system, you have lost operational control.

A defensible programme therefore includes data and algorithmic portability. At a minimum, you should be able to export your feature definitions, model documentation, and decision logs in usable form. You should know which parts of your pipeline are proprietary and which parts are replaceable. You should also be able to demonstrate that you evaluated vendor risk and monitored vendor changes as part of your governance function.

Visibility is equally important. In an agent ecosystem, your systems interact with vendor agents and customer agents in ways that can create emergent behaviour. If you cannot see those interactions and reconstruct them later, you cannot explain them. Under regimes emphasising transparency and accountability, that

lack of visibility becomes a compliance failure, not merely a technical inconvenience.

What is Your Story: Can You Explain Your AI Programme to a Regulator, Legislator, or Judge?

The most persuasive compliance posture is a coherent story backed by evidence. Your story should be consistent across privacy, cybersecurity, and AI governance. It should also be consistent across technical and legal audiences. The NIST AI RMF is useful here because it gives you a vocabulary for governance, risk mapping, measurement, and management that can be translated into board-level reporting and into regulator-facing documentation.

A credible story typically includes the following elements:

- You defined the purpose of the AI system and limited data processing to that purpose.
- You used data minimisation and retention discipline, including secure disposal.
- You documented model inputs, intended use, limitations, and monitoring.
- You implemented human oversight where it mattered.
- You evaluated foreseeable risks, including discrimination risk and security risk, and mitigated them.
- You retained evidence of decisions and changes so you could reconstruct what happened.

These elements track directly to themes in Colorado's statute around reasonable care, documentation, and impact assessments, and to the EU AI Act's emphasis on documentation and transparency. They also track to the FTC's framing of security as collecting only what you need, protecting it, and disposing of it.

The point is not to memorise a framework. The point is to build an operational system of proof. When the question comes, you answer with documents, logs, testing artifacts, and governance records, not with aspiration.

Practical Guardrails for the "Data-Light AI" Future

Below are guardrails that high-level counsel can insist on without pretending to be engineers. They are prin-

ciples that translate into controls, and they can be audited.

Guardrail 1: Collect less, keep less, and prove it

Create retention schedules that are actually enforced technically, not just written. Build deletion into pipelines and verify it. Use the FTC’s “scale-down” logic as a simple executive narrative: keep only what you need and dispose of the rest securely.

Guardrail 2: Treat models and prompts as regulated assets

Maintain a registry of models, prompts, tools, and agents used in production. Document intended use and prohibitions. Require change control for material updates, especially when outputs drive consumer interactions or decisions.

Guardrail 3: Require explainability that matches the risk

Not every system needs deep interpretability. High-risk and consequential contexts do require a stronger ability to explain outputs, document inputs, and show oversight. Risk-based governance is the theme across modern AI regulation and frameworks.

Guardrail 4: Build portability and exit options into procurement

Contract for access to logs, documentation, and exportable artifacts. Avoid architectures where you cannot migrate feature stores or decision logic. Portability is not a luxury in an enforcement environment.

Guardrail 5: Use privacy-enhancing technologies where they reduce exposure without erasing accountability

Differential privacy, federated learning, secure computation, and encryption can reduce exposure, but they do not eliminate governance needs. Use them as part of a measured programme, and document why you used them and what tradeoffs you accepted.

The Competitive Advantage Is Not Data; It Is Governed Adaptability

AI and agents will reduce the business need to retain detailed personal data in many contexts, and they will expand the ability to test markets and personalise experiences. The legal and security risks do not disappear. They relocate to models, to supply chains, to explainability, and to governance.

A winning organisation will be able to say, with evidence, that it designed for minimal retention, strong security, and rapid change. It will be able to show that it can modify policy and technical controls quickly without calling outside contractors for every change. It will be able to explain to a regulator or jury how the system worked, what was foreseeable, and why the choices were reasonable. That is the “one story” approach, and it is the most durable strategy you can buy in an unpredictable world.

USA – UTAH



Trends and Developments

Contributed by:

Clifford Blair

Kirton McConkie

Kirton McConkie is Utah's premier multi-service law firm, with over 200 attorneys across five offices. It offers practical legal service to clients in all 50 states and in more than 150 countries. The firm's practice areas span data privacy, intellectual property law, corporate law, real estate law and litigation. Its attorneys are trusted advisers, strategic problem-solvers and true partners to clients. With graduates from 52

different law schools, including nine of the top ten US law schools, the legal team brings a broad range of experience, insight and industry knowledge to every case. Nearly half of the firm's attorneys speak multiple languages, and many have practised law internationally, giving it the perspective and capability needed to handle legal matters across borders and industries.

Author



Clifford Blair is a member of Kirton McConkie's international section and head of its privacy practice. He advises domestic and foreign businesses and non-profits about all aspects of international business,

especially compliance. Mr Blair helps organisations build practical privacy programmes that scale across jurisdictions. He advises on data protection regimes around the world and is a trusted adviser on complex global data breaches, having guided clients through reporting obligations in virtually every country. Mr Blair previously served as in-house counsel for the International Monetary Fund and as a litigator in New York, focusing on international arbitration and transnational litigation issues.

Kirton McConkie

36 S. State St., Ste. 1900
Salt Lake City
UT 84111
USA

Tel: +1 801 328 3600
Email: cblair@kmclaw.com
Web: www.kirtonmcconkie.com

KIRTON | McCONKIE

Utah Privacy Law in 2026: A Practical and Strategic Guide for Businesses

Utah privacy law has developed rapidly in recent years, but the Utah Consumer Privacy Act remains the foundation of the state's comprehensive privacy framework. At the same time, the Utah Legislature has enacted additional statutes addressing artificial intelligence (AI), cybersecurity, social media governance, electronic data access and digital identity infrastructure.

For organisations operating in Utah or serving Utah residents, privacy compliance is no longer a discrete legal project but an ongoing regulatory responsibility touching marketing, product design, information security, vendor management and customer service. With the 2026 state legislative session ongoing, further changes to Utah's privacy law should be expected.

Utah's Place in the US Privacy Landscape

When the Utah Consumer Privacy Act was signed on 24 March 2022, Utah became just the fourth US state to enact comprehensive consumer privacy legislation, following California, Colorado and Virginia. The Act entered into force on 31 December 2023.

Utah adopted a pragmatic structure from the outset. Enforcement authority rests with the attorney general rather than private litigants and the statute avoids broad rule-making authority. Applicability thresholds are designed to focus on medium and large organisations. While the Utah Consumer Privacy Act shares many similarities with Colorado and Virginia law, compliance requires careful analysis for organisations operating in multiple jurisdictions, as there are differences.

Scope of Application: Revenue and Data Thresholds

The Utah Consumer Privacy Act applies to for-profit entities conducting business in Utah or targeting Utah residents that meet both a revenue and data-processing threshold. The statute applies to organisations with annual revenue exceeding USD25 million that either:

- control or process personal data of 100,000 or more Utah consumers during a calendar year; or

- control or process personal data of 25,000 or more Utah consumers and derive more than 50% of gross revenue from the sale of personal data.

Utah's USD25 million revenue threshold is absolute. If it is not met, the statute does not apply, regardless of consumer volume. This differs from California and Colorado, where revenue is not always a gating requirement.

Exemptions apply to governmental entities, institutions of higher education, non-profit organisations, indigenous tribes, and personal data regulated under federal statutes such as the Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act of 1999 and the Fair Credit Reporting Act of 1970. Organisations that are uncertain about the applicability of the Utah Consumer Privacy Act should document their analysis of revenue calculations, consumer counts and monetisation practices.

Personal Data and Sensitive Data

Personal data under the Utah Consumer Privacy Act includes information linked or reasonably linkable to an identifiable individual. This definition captures common business data, including:

- names and contact details;
- account credentials;
- online identifiers and device information;
- transaction histories; and
- location data.

The Act also defines sensitive data, including information revealing:

- racial or ethnic origin;
- religious beliefs;
- sexual orientation;
- citizenship or immigration status;
- health conditions;
- genetic or biometric data; and
- precise geolocation.

Before processing sensitive data, controllers must provide clear notice and an opportunity to opt out. Organisations should evaluate marketing tools, ana-

lytics platforms and AI systems to determine whether sensitive data is implicated directly or indirectly.

Definition of “Sale” and Competitive Clarity

Utah defines “sale” narrowly as the exchange of personal data for monetary consideration. This approach contrasts with California’s broader “monetary or other valuable consideration” standard. Utah further excludes disclosures consistent with a consumer’s reasonable expectations. This narrower construction reduces ambiguity for organisations engaged in analytics, cross-context advertising, or vendor partnerships. However, multi-state operators must remain cautious. Practices that fall outside Utah’s definition may still constitute a sale under California or Colorado law.

Controllers and Processors: Allocation of Duties and Vendor Management

As is common in many privacy statutes around the world, the Utah Consumer Privacy Act distinguishes between controllers and processors and uses definitions similar to other jurisdictions: controllers determine the purposes and means of processing personal data, while processors act on behalf of controllers pursuant to written instructions.

Organisations sharing personal data with vendors, service providers or other third-parties should have contracts in place governing the data. Such controller-processor contracts must:

- describe the nature and purpose of processing;
- impose confidentiality obligations;
- require reasonable administrative, technical and physical safeguards; and
- ensure that subcontractors provide equivalent protections.

Periodic review of processor agreements and due diligence documentation strengthens defensibility in the event of regulatory scrutiny of such data sharing.

Consumer Rights and Operational Demands

Utah consumers possess defined rights under the Utah Consumer Privacy Act. Controllers must implement structured workflows to receive, verify and

respond to requests efficiently. Consumers have the right to:

- confirm whether personal data is processed and access that data;
- delete personal data provided by the consumer;
- obtain a portable copy of previously provided data;
- opt out of targeted advertising or the sale of personal data; and
- correct inaccurate personal data (effective 1 July 2026).

The right of correction, effective 1 July 2026, requires particular attention. Correction requests may necessitate updates across multiple systems. Organisations should define internal criteria for evaluating such requests and document implementation decisions. Controllers must respond to data subject rights requests within 45 days. A single 45-day extension is permitted when reasonably necessary. In the case of data subject complaints or regulatory investigations, the Attorney General must provide written notice and a 30-day opportunity to cure before enforcement action, as discussed in more detail below.

Transparency and Privacy Notices

Transparency is an important element in Utah privacy law, as in other jurisdictions. Controllers must provide consumers with a reasonably accessible privacy notice describing:

- categories of personal data processed;
- purposes of processing;
- categories of third parties receiving data; and
- available consumer rights and methods for exercising them.

Overly generic disclosures risk undermining statutory transparency obligations. Regular review is advisable, particularly when deploying new technologies or modifying vendor relationships.

Data Minimisation and Security Practices

Although the Utah Consumer Privacy Act does not use the term data minimisation explicitly, responsible data governance remains essential. Collecting only the data necessary for defined business purposes reduces risk exposure and simplifies compliance obligations. The

Act requires organisations to implement reasonable administrative, technical and physical security safeguards. Strong security controls also support incident response readiness. Breach response planning should include defined roles, communication protocols and documentation procedures.

Enforcement Structure and Cure Provisions

Utah employs a hybrid enforcement model. The Utah Division of Consumer Protection investigates complaints and refers matters to the Attorney General. The Attorney General has exclusive authority to bring enforcement actions. If a violation is identified, the Attorney General must provide written notice and a 30-day opportunity to cure. Civil penalties may reach USD7,500 per violation for uncured violations.

Unlike California (but similar to Colorado and Virginia), Utah provides no private right of action under the Utah Consumer Privacy Act. Utah also has no standalone dedicated enforcement agency for privacy, as does California. Notably, neither the Division of Consumer Protection nor the Attorney General is empowered to promulgate privacy regulations. This absence provides predictability for organisations subject to the statute.

Cybersecurity and Breach Co-Ordination: Senate Bill 127

Following the adoption of the Utah Consumer Privacy Act, in 2023 the Utah Legislature passed Senate Bill 127, which strengthens breach notification and cybersecurity governance in Utah. Entities owning or licensing computerised personal data must investigate suspected breaches and provide timely notice where misuse for identity theft or fraud is confirmed. Breaches of relevant data affecting 500 or more residents must be reported to the Attorney General and the Utah Cyber Center. Data covered by the breach notification requirement is similar to other US jurisdictions and is limited to Social Security number, driver licence or State Identification number, and financial account information that would permit access to the account. Governmental entities must report breaches to the Utah Cyber Center.

The Utah Cyber Center co-ordinates statewide cybersecurity planning, incident response, and threat infor-

mation sharing. From 1 January 2025, governmental entities must generally use authorised top-level domains such as.gov,.edu or.mil for official communications, subject to limited exceptions. These measures illustrate Utah's investment in structured cybersecurity infrastructure.

Electronic Information and Law Enforcement: Senate Bill 226

In the year after the adoption of the Utah Consumer Privacy Act, the legislature strengthened privacy protections in the context of law enforcement by adopting Senate Bill 226, which limits access to electronic data. Law enforcement agencies must obtain a search warrant based on probable cause before accessing location information, stored data or transmitted data from electronic devices, except in defined emergency or consent-based circumstances. Data not covered by a warrant must be destroyed in an unrecoverable manner. Agencies may not use, copy or disclose information outside the scope of the warrant, subject to narrow exceptions. The statute protects providers acting in good faith reliance on a warrant from liability. The statute reinforces judicial oversight and aligns Utah more closely with global expectations regarding digital privacy safeguards.

Social Media Regulation and Youth Protection

Utah has been at the forefront among US states in regulating social media platforms, particularly with respect to minors; however, Utah's efforts have been marked by sustained legislative action and ongoing constitutional litigation. In March 2023, the Utah Legislature enacted the Utah Social Media Regulation Act through SB 152 and HB 311, imposing age verification, parental consent requirements, advertising restrictions, and limits on certain platform features. Those provisions were challenged on constitutional grounds and ultimately repealed and replaced in 2024 with a revised framework, including the Minor Protection in Social Media Act (SB 194/HB 464), which was designed to refine age-assurance systems, strengthen default privacy protections, restrict features such as autoplay, and provide supervisory tools for parents.

The revised law was scheduled to take effect on 1 October 2024, but on 10 September 2024 a federal district court granted a preliminary injunction block-

ing its implementation, concluding that Utah had not demonstrated that the statute was likely to withstand First Amendment scrutiny, notwithstanding the state's interest in protecting minors. The related litigation, most prominently *NetChoice v Reyes*, remains ongoing. Most recently, the state urged the Tenth Circuit Court of Appeals to reinstate the law, arguing that it regulates structural platform features rather than protected speech. Members of the appellate panel questioned whether the statute can meaningfully distinguish between regulated design features and constitutionally protected expression. As a result of the litigation, no social media age-verification or platform-design restrictions are currently enforceable in Utah while the legal challenges proceed.

The Artificial Intelligence Policy Act and AI Governance

Utah's Artificial Intelligence Policy Act, effective 1 May 2024, established the Office of Artificial Intelligence Policy and the Artificial Intelligence Learning Laboratory Programme. The Learning Laboratory permits regulatory mitigation agreements for AI innovators operating under defined safeguards, including the possibility of limited exceptions from certain state-level regulatory requirements. Participants must demonstrate technical competence, financial capacity and effective risk management plans, and are required to report incidents promptly and to comply with cybersecurity auditing procedures.

In addition to creating this innovation-focused framework, Utah's AI legislation emphasises transparency at consumer-facing touchpoints. Businesses must disclose when individuals are interacting with AI systems, such as chatbots or automated service tools. Certain high-risk applications, including AI tools used in sensitive contexts such as mental health support, are subject to additional restrictions relating to advertising practices, data use and consent.

Although the Artificial Intelligence Policy Act encourages innovation through regulatory mitigation, it also clarifies that existing consumer protection laws apply to AI applications. Organisations deploying AI should therefore integrate AI governance into broader privacy and compliance frameworks. Practical steps include:

- inventorying AI systems currently in use;
- evaluating whether consumer disclosures are required;
- implementing structured review mechanisms for higher-risk applications; and
- maintaining documentation of AI-related decision-making processes.

Utah's approach reflects a dual objective: promoting responsible innovation while embedding oversight where consumer risk is most acute.

The 2025 Legislative Session: Recent Legislative Developments

While the Utah Consumer Privacy Act remains the foundation of Utah's privacy framework, the Utah Legislature has continued to refine and expand the state's approach to data governance. Since the Utah Consumer Privacy Act's adoption in 2022, lawmakers have enacted and amended statutes addressing cybersecurity co-ordination, electronic data access, social media governance and AI oversight. Together, these measures create a layered regulatory environment in which privacy, security and consumer protection intersect.

The 2025 legislative session expanded Utah's privacy framework beyond the Utah Consumer Privacy Act, with lawmakers introducing measures that address government data governance and AI transparency. These changes reflect how Utah is increasingly treating privacy as a cross-cutting issue with a broader view of privacy risk.

Changes to AI policy

In 2025, the Utah Legislature amended the Artificial Intelligence Policy Act to refine and extend its regulatory framework. Under the follow-on legislation signed in the 2025 General Session, including Senate Bill 226 and Senate Bill 332, the scope and requirements of the act were narrowed and clarified, and the act's sunset date was extended until 1 July 2027. These amendments focus the AI disclosure obligations on instances where consumers make a clear and unambiguous request to know whether they are interacting with AI and limit proactive disclosure obligations for high-risk interactions involving sensitive personal or regulated occupational data. In addition, the legisla-

ture enacted complementary provisions addressing mental health chatbots and expanded protections against unauthorised AI-generated impersonations. These changes tailor Utah's AI regulatory environment towards more specific consumer protection contexts while maintaining an innovation-friendly posture.

Strengthened oversight of government agencies

House Bill 444 strengthened privacy oversight within state government. It increased the authority of the Utah Privacy Commission and clarified rules governing how agencies collect and use personal data. For example, government websites must include plain-language privacy notices. Agencies must also identify high-risk data practices, such as facial recognition and automated profiling. Contractors working with state agencies must comply with similar standards. Organisations that provide services to the government should review contractual privacy provisions carefully and ensure alignment with statutory expectations.

The 2026 Legislative Session: Ongoing Developments (as of 20 February 2026)

Utah's 2026 General Session is ongoing, and several introduced measures would materially affect cybersecurity co-ordination and AI oversight. Because bills may be amended during the session, organisations should track both the substance and the direction of travel: the proposals collectively signal continued legislative interest in technology governance, accountability and risk controls.

State-endorsed digital identity programme (SB 275)

Senate Bill 275 would create a state-endorsed digital identity programme and, notably, would establish a statutory digital identity bill of rights. The bill's text frames core principles around individual control, voluntariness (including a right not to be compelled by the state to use a digital identity in place of a physical credential), transparency in design and operation, and protections against surveillance or persistent monitoring except as authorised by law.

The proposal would also set out requirements and responsibilities for multiple participants in the ecosystem (including governmental entities and private-sector participants, such as digital wallet providers,

verifiers and relying parties), and includes enforcement and complaint pathways. In practice, if enacted, Senate Bill 275 could become a key “plumbing” statute for identity-related privacy in Utah, with downstream implications for authentication, attribute sharing and data-handling expectations across services that choose to recognise state-endorsed credentials.

AI transparency amendments (HB 286)

House Bill 286 would enact an AI Transparency Act aimed at “frontier” AI models. The bill would require developers of certain covered models to create and publish public safety and child protection plans, publish summaries of risk assessments, and report certain safety incidents to the Office of Artificial Intelligence Policy. The proposal also includes civil penalties and employee whistle-blower protections tied to reporting safety concerns.

AI amendments (HB 438)

House Bill 438 would enact an AI Companion Chatbot Safety Act to regulate AI companion chatbots and protect consumers. The bill's highlighted provisions include requiring suppliers to implement safety protocols (and assess their efficacy), facilitate independent evaluation, and publicly report on safety protocols and related metrics. It would also give the Office of Artificial Intelligence Policy authority to establish disclosure standards and monitor compliance, and it proposes restrictions that are directly privacy-adjacent, including limits on selling or sharing highly sensitive information and additional protections involving minors. As drafted, HB 438 reflects Utah's continued pattern of regulating AI at specific consumer-risk touchpoints rather than attempting to impose a single, omnibus AI framework.

Government cybersecurity amendments (SB 123)

Senate Bill 123 would affect government cybersecurity by modifying provisions related to the Utah Cyber Center. The highlighted provisions include expanding the Cyber Center's duties to include local education agencies, adjusting deadlines for statewide strategic cybersecurity planning, making changes to the composition of the Cybersecurity Commission, and creating a restricted account for the Cyber Center.

For organisations that interact with public-sector systems, the practical takeaway is that Utah continues to formalise the state’s cybersecurity co-ordination model – potentially affecting expectations around collaboration, reporting and incident-response support structures when an event touches government networks or partners.

Public sector privacy amendments (HB 450)

House Bill 450 focuses on Utah’s public-sector privacy framework. The bill would amend the Government Data Privacy Act and also makes related changes to the statute on public access to records. HB 450 would restructure elements of Utah’s privacy governance infrastructure, including changes involving the Utah Privacy Commission and the Office of Data Privacy (such as transferring support functions). It further proposes to establish the data privacy ombudsman as a component of the Office of Data Privacy, and it would expand amendment and correction procedures to cover information beyond “personal data” in the public-sector framework. A central feature is stronger process and oversight around certain “high-risk” governmental technologies (including provisions addressing authorisation before implementing specified surveillance-related activities, and reporting/oversight mechanisms tied to those activities).

Conclusion

Utah privacy legislation reflects incremental development of privacy law at the state level in the USA. The Utah Consumer Privacy Act establishes core consumer rights and enforcement mechanisms. Subsequent legislation addressing cybersecurity, electronic data access, AI and social media governance has expanded the state’s regulatory ecosystem. With the 2026 legislative session ongoing, further refinements are possible. Organisations that maintain disciplined, well-documented and adaptable compliance programmes will be best positioned to respond to any changes effectively while preserving consumer trust and operational resilience.

USA – WASHINGTON



Trends and Developments

Contributed by:

Amy Weston, Eva Novick, Brian Esler and Lauren Fricke
Miller Nash LLP

Miller Nash LLP is a nationally recognised, industry-focused law firm with offices in Alaska, California, Idaho, Oregon and Washington. The firm advises clients on privacy and data security in a rapidly evolving regulatory and threat landscape. Miller Nash helps organisations navigate a patchwork of state, federal and international requirements, including Washington's My Health My Data Act, the California Consumer Privacy Act, the General Data Protection Regulation, the Telephone Consumer Protection Act, the Gramm Leach Bliley Act, and the Family Educational Rights and Privacy Act. The team drafts and updates pri-

vacancy notices, designs data governance programmes, and conducts data protection audits that align with business objectives. When incidents occur, Miller Nash guides organisations through breach response, regulatory inquiries and related legal obligations, and defends companies in litigation. The team also reviews and negotiates vendor contracts, including cloud computing, information technology, artificial intelligence, networking, data centre and database agreements in domestic and international transactions.

Authors



Amy Weston is a partner at Miller Nash LLP, where she advises clients on complex commercial transactions with a particular focus on technology, data protection and privacy. In addition to her commercial practice,

Amy guides clients through all stages of the corporate life cycle, including formation, governance, debt and equity financings, and mergers and acquisitions, with a strong emphasis on information security and privacy. Whether advising United States-based emerging companies or well-established global corporations, she helps clients navigate the nuances of domestic and international data protection and privacy laws, developing practical strategies to safeguard proprietary inventions, systems, processes and sensitive information.



Eva Novick is a partner at Miller Nash LLP and a Certified Information Privacy Professional (AIGP, CIPP/US, CIPP/E, CIPM) who leads the firm's privacy and data security team. With nearly two decades at the Oregon

Department of Justice (DOJ) before private practice, she advises businesses on US and international

privacy compliance, including CCPA/CPRA and GDPR, and incident response. She represents clients in privacy-related litigation, including class actions involving data breaches and tracking technologies. At the DOJ, she led multistate investigations, resolving more than 400 matters and securing over USD1 billion in restitution.



Brian Esler is a partner at Miller Nash LLP whose practice focuses on complex business litigation, intellectual property disputes, construction litigation, financial institution defence and appellate

advocacy. He has tried and argued cases in state, federal and tribal courts, as well as before arbitrators and administrative agencies, and has briefed and argued appeals in the Washington Court of Appeals, the Washington Supreme Court and the Ninth Circuit. Brian is highly regarded for his litigation skill and strategic advocacy, and has received numerous honours recognising his excellence in the field. He formerly co-chaired the ABA Section of Litigation's Business Torts and Unfair Competition Committee, and is currently a member of the Section's Content Management Committee.

Contributed by: Amy Weston, Eva Novick, Brian Esler and Lauren Fricke, **Miller Nash LLP**



Lauren Fricke is an associate on Miller Nash's business and corporate team. She advises clients at all stages of growth on contract negotiations, technology transactions, mergers and acquisitions, and privacy and data

protection matters. Lauren works with emerging companies and established national and international organisations, providing practical, business-focused guidance. Holding both a JD and an MBA, she delivers strategic counsel aligned with each client's operational and long-term objectives.

Miller Nash LLP

605 5th Ave S, Ste 900
Seattle, WA 98104
USA

Tel: +1 206 624 8300
Fax: +1 206 340 9599
Email: ClientServices@MillerNash.com
Web: www.millernash.com



Navigating Data Privacy in Washington State: A 2026 Outlook for Businesses

Introduction

For Washington businesses, data privacy has evolved beyond a technical concern to become a central legal and operational reality. The landscape in 2026 is defined by significant new laws, aggressive enforcement and a surge in private lawsuits. This article examines the key trends driving that shift, helping organisations understand both the legal requirements and the practical steps needed to thrive. Complex legal developments are distilled into clear, actionable insights for business leaders and operational teams, offering organisations a roadmap for the coming year's critical compliance and risk management priorities.

Key Legal and Regulatory Updates for 2026

Washington's regulatory environment has solidified with the full implementation and maturation of several key laws. The Washington My Health My Data Act (MHMDA) remains a cornerstone, but its interpretation by the Attorney General's office has clarified several previously ambiguous points. Furthermore, though Washington's first-of-its-kind "Washington Privacy Act" was never passed, businesses in Washington are now operating under its functional equivalent thanks to a combination of sector-specific rules, aggressive application of the Consumer Protection Act (CPA) to data practices, and other states having used the Washington Privacy Act as the basis of their comprehensive state privacy law.

The most significant development is the expansion of "health data" definitions under the MHMDA and related laws. The Washington Attorney General's office and private plaintiffs can now enforce an administratively broadened law and focus on a wide array of computer-generated information rather than just traditional medical records. This expansion directly impacts businesses far beyond the healthcare sector.

- Newly included data types: purchase histories for supplements, fitness tracker data, search queries related to medical symptoms, and wellness app information (even from general mindfulness apps) are now routinely treated as protected health data.
- Geofencing restrictions: the use of geofencing technology to identify and target consumers near

healthcare facilities is now virtually prohibited, with severe penalties for violations.

- Universal consumer rights: inspired by broader trends, Washington now expects all businesses, regardless of size or sector, to honour core consumer rights for health data – the right to access, delete and correct their personal data, and to opt out of its sale.

Plaintiff attorneys are actively leveraging the CPA to protect consumer rights and enforce compliance with privacy laws. Courts now construe the CPA to grant consumers rights such as the right to access, correct, delete and opt out of the sale of their personal data, and to require businesses to be transparent about their data practices and to limit data collection to necessary purposes. With litigants able to recover attorneys' fees and treble damages for violations, the CPA offers a significant financial incentive for plaintiff attorneys.

Emerging Litigation Trends: Where the Legal Battles Are Happening

Litigation is no longer dominated solely by regulatory actions. A thriving ecosystem of private plaintiff lawsuits has emerged and extends well beyond the MHMDA's private right of action. These cases are setting costly precedents and creating new liabilities. The plaintiff's bar has become sophisticated in identifying technical violations that can lead to statutory damages, which can quickly scale for large customer bases. Some of the more common claims include the following.

- Failure to have a health data privacy notice: the MHMDA requires a separate health data privacy notice in addition to the general website privacy notice.
- Collection of health data without consent: tracking technologies collecting information about a visit to certain websites or products/services contained on those websites without affirmative express consent are a violation of the MHMDA. See further below regarding implied consent challenges.
- Sharing health data: similarly, "sharing" or "selling" health data to third parties, such as website analytics providers, without authorisation can be problematic.

Additionally, these cases rarely rely only on the MHMDA and typically incorporate other causes of action.

Another major trend is the rise of “dark pattern” litigation. Plaintiffs’ attorneys are successfully arguing that website designs and user interfaces that make it difficult to find privacy controls or that nudge users towards sharing data constitute unfair or deceptive practices under the CPA. Simply having a privacy notice is no longer a defence if the actual user experience contradicts disclosures or hides consumer choices.

- Examples of alleged “dark patterns”: buried consent buttons, pre-checked boxes for data sharing, confusing toggle switches, and requiring account creation to exercise data rights.
- Implied consent challenges: businesses that claim “implied consent” from continued website use are losing cases, as courts demand clear, affirmative and unbundled consent for data collection and sharing.
- Vendor liability: lawsuits increasingly name both the primary business and its third-party data processors (such as analytics or marketing vendors), arguing shared responsibility for unlawful data flows.

In parallel with the trends described above, businesses should expect expansive privacy litigation around AI-driven profiling and automated decision-making that leverage broad categories of “health data”, including purchase histories for supplements, fitness tracker outputs, symptom-related search queries, and wellness app information, all of which are now routinely treated as protected. This expansion heightens discrimination and bias risk for businesses that deploy machine-learning models in marketing, personalisation or eligibility determinations, because allegedly biased inferences or opaque data flows can be framed as unlawful “collection”, “sharing”, or “sale” of health data without clear, affirmative and unbundled consent. Implicit in the “dark patterns” litigation described above is the argument that confusing consent flows or buried controls render algorithmic processing non-transparent or deceptive. Litigants are increasingly targeting both the primary business and its analytics or marketing vendors under shared-responsibility the-

ories. Businesses should expect courts and regulators to assess the reasonableness of governance over AI tools (including vendor use of business data to train models) and to treat vendor practices as extensions of the business, reinforcing the need for contractual audit rights and alignment between disclosures and actual data flows.

Businesses can further expect fallout from the 2026 Washington Supreme Court ruling in *Brown v Old Navy* (2:23-cv-00781-JHC) that advertisers cannot send emails that contain any false or misleading information in the email subject line. *Brown* expands the scope of Washington’s anti-spam law, the Commercial Electronic Mail Act (CEMA). CEMA was passed in 1998 to address the influx of unsolicited, deceptive or misleading commercial emails received by Washington consumers. The court in *Brown* construed the law broadly, holding that it prohibits *any* false or misleading information in the subject line, even information that only misrepresents the commercial nature of the message such as “Today Only” or “Three Days Only” for a sale that in fact lasts longer than advertised. Washington businesses should exercise caution when relying on their email marketing vendors to ensure compliance with anti-spam laws. Most vendors are familiar with the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), but CAN-SPAM does not pre-empt state laws that prohibit material falsity or deception in any portion of a commercial email. Businesses now face penalties of up to USD500 per violation or actual damages, whichever is greater, if their email subject line creates a false sense of urgency about discounts.

As is the case elsewhere, the plaintiffs’ bar in Washington is actively monitoring data breach reports, searching out affected individuals, and filing follow-on class action complaints. Evolving Washington case law has recognised potential common law duties to safeguard information, and that organisations that manage greater amounts of sensitive data have a correspondingly greater duty to safeguard that information. Organisations in particular sectors that are known to be targeted by data thieves (such as healthcare and education) may be particularly easy targets for plaintiff class action lawyers, since the evolving case law seems to assume that entities in those sectors

know of the risk and should implement correspondingly greater security measures. Class action lawyers are also becoming more creative in the claims they plead, evolving from mere negligence allegations to claims of breach of contract, breach of fiduciary duty, and violations of Washington's CPA, which allows for recovery of fees and treble damages.

Furthermore, Washington businesses need to be mindful of privacy class actions that have been sweeping across the country. For example, Washington businesses that do not do business with consumers in other states or only operate business to business (B2B) may still be served with a complaint alleging various state and federal theories, such as under the California Invasion of Privacy Act (CIPA), the Electronic Communications Privacy Act (ECPA) and the Video Privacy Protection Act (VPPA). Businesses should also continue to monitor laws enacted in other states, such as Maryland's new Online Data Privacy Act (MODPA), which requires businesses of a certain size to obtain explicit consent from individuals before collecting or sharing their precise location information. Designed to prevent unauthorised tracking or surveillance, MODPA encompasses information obtained from GPS, Wi-Fi, Bluetooth, cellular tower triangulation or similar technologies. MODPA's geolocation restrictions mirror the geofencing limitations in the MHMDA, and businesses can and should expect Washington courts and regulators to take note of how MODPA is enforced and interpreted in Maryland.

While there is currently no Washington law involving children's data or requirements of age-appropriate website or app design, businesses can expect a greater focus on children's privacy under other state and potentially federal legal initiatives. Similarly, Washington businesses will face challenges and risks when handling personal data of non-Washington residents, as the patchwork collection of state comprehensive and sector-specific privacy laws continues to grow.

Washington businesses can protect themselves by having an updated and accurate website privacy notice, obtaining consent through a cookie banner that is properly operating, avoiding dark patterns, tightening their vendor contracts, and continuously monitoring their security protocols so as to have an

auditable paper trail of best practices should data thieves strike and class action lawyers follow.

Top Compliance Challenges for Businesses

Moving beyond understanding the law, the practical task of compliance presents several consistent challenges. First is the mapping and inventory dilemma. Many organisations still lack a clear, real-time picture of what data they collect, where it flows and with whom it is shared. This foundational gap makes complying with access, deletion and opt-out requests operationally impossible.

Secondly, the vendor management life cycle has become a high-stakes compliance area. The old practice of signing a vendor's standard data agreement is now a major liability. Businesses must actively manage their third-party relationship with ongoing diligence and enforceable contractual protections that match regulatory duties. In addition to verifying that vendors do not share, sell or otherwise use customer data or personal information for their own purposes, businesses must grapple with the risk of vendors using business data to train AI tools. Contractual restrictions, even if legally enforceable against the vendor, may not offer a satisfactory defence if a customer's data is leaked or otherwise disclosed due to a vendor's failure to follow its own promises. Businesses should take steps to assess their vendors' cybersecurity and privacy compliance systems, and should reserve the right to audit a vendor's tools to ensure that their promises match what their contracts say.

Finally, incident response preparedness has shifted. The legal standard is no longer just about notifying authorities after a breach. Regulators and plaintiffs examine the *reasonableness* of data security practices *before* the incident. Documented privacy impact assessments, regular employee training, and encryption standards are scrutinised to determine whether negligence occurred. What was considered "reasonable" five or ten years ago is no longer reasonable; data security practices must be regularly reviewed and updated to take into account changing technologies and risk vectors.

Actionable Recommendations for 2026

Conduct a “Privacy Maturity Audit”

This goes beyond a data map to assess policies, vendor contracts, website user experience, and employee training against current enforcement priorities. Review retention and deletion schedules to ensure data minimisation over time. Develop detailed, test incident response “playbooks” and conduct tabletop exercises. Consider routine privacy impact assessments for all new products, marketing initiatives and vendor onboarding to align with the evolving “reasonableness” standard. The goal is not perfection – it is prioritisation. Identify your single greatest compliance gap and draft a concrete remediation plan to address it immediately with defined ownership and timelines.

Review your vendor contracts

Next, revamp your vendor contracts. Ensure that every agreement with a service provider that touches personal data includes explicit requirements for:

- assisting with consumer rights requests;
- mandatory breach notification; and
- the right to audit vendor compliance.

Regulators increasingly treat vendor practices as an extension of the business itself, and enforcement actions reflect that reality. Although Washington does not have specific statutory requirements for vendor contracts outside the MHMDA, Washington businesses can leverage broader requirements in other state privacy laws for a standard vendor contract framework.

Design privacy interfaces defensively and transparently

Implement clear, layered and consumer-friendly privacy interfaces. Design your website and app privacy controls with the assumption that they will be exhibits in a court proceeding. Use plain language, make opt-out paths as easy as opt-in, and document all consumer choices meticulously. Well-designed interfaces are not just compliance tools – they are reputational safeguards.

Immediate priority checklist

- Audit all website and app user flows for potential “dark patterns”.
- Designate a point person responsible for responding to consumer rights requests within the legally mandated timelines, and implement practical steps for verifying requestor identity and handling fraudulent rights requests.
- Update breach response plans to include scenarios involving the broadened definition of health data.
- Schedule annual privacy training for all employees, with specialised training for marketing and product development teams.
- Conduct regular audits of security practices to establish a pattern of best practices.
- Put in place regular, and no less frequently than annual, review of privacy notices and internal policies.

Conclusion: Building Trust as a Competitive Advantage

The data privacy landscape in Washington for 2026 is complex, but also presents an opportunity. Organisations that view privacy compliance merely as a legal burden will struggle with costs and litigation. Given the Attorney General’s enforcement posture, the availability of attorneys’ fees and treble damages, and evolving expectations that businesses honour universal consumer rights to access, delete, correct and opt out of the sale of health data, companies face material exposure if they cannot demonstrate explainability, auditable consent, vendor oversight, and defensible design of privacy interfaces for AI-related and traditional processing. Companies that proactively adopt transparent and respectful data practices will build deeper trust with their customers. This trust is becoming a measurable competitive differentiator. By investing in robust privacy programmes now, companies are not just avoiding fines but are also future-proofing business operations, enhancing brand reputation and fostering lasting customer loyalty in an era where data stewardship is paramount.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com