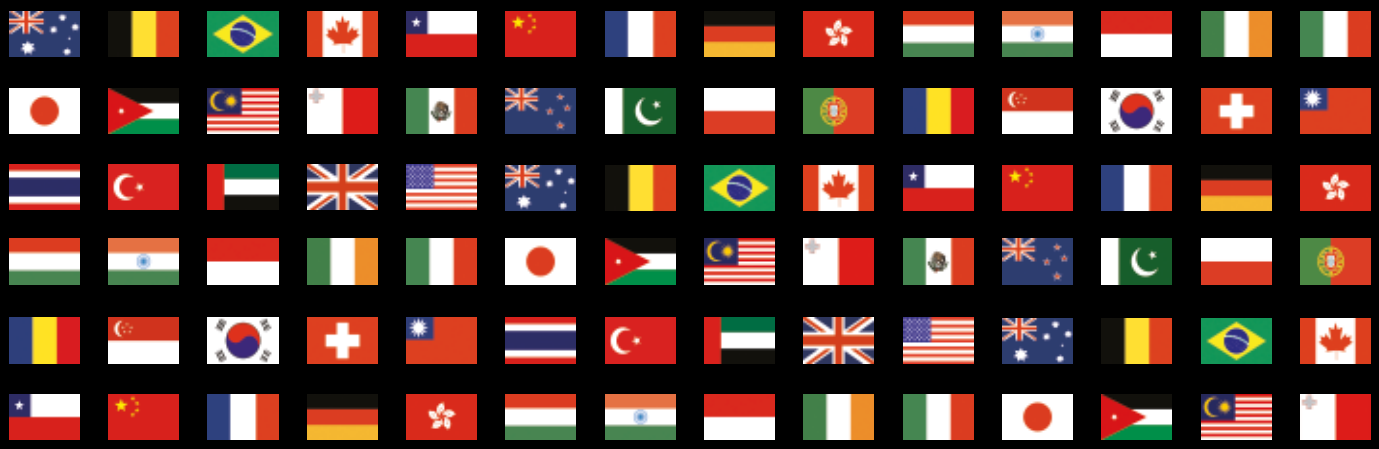
DATA PROTECTION & PRIVACY 2023

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP



LEXOLOGY
Getting the Deal Through

HUNTON
ANDREWS KURTH

HUNTON
ANDREWS KURTH

Leaders in Privacy and Cybersecurity

Keep the trust you've earned.

Complying with global privacy, data protection and cybersecurity rules is challenging, especially for businesses that operate across borders. Our top-ranked privacy team, in combination with the firm's Centre for Information Policy Leadership, advises on all aspects of US and European data protection law and cybersecurity events. We help businesses develop global compliance frameworks addressing regulatory obligations in the US, the EU and across the world. The firm is widely recognized globally as a leading privacy and data security firm.

For more information, visit www.huntonprivacyblog.com.

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Eleventh edition
ISBN 978-1-83862-997-7

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

DATA PROTECTION & PRIVACY 2023

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting the Deal Through is delighted to publish the eleventh edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting the Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on South Korea and United Arab Emirates.

Lexology Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting the Deal Through

London
July 2022

Contents

Introduction

Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

This introduction aims to highlight the main developments in the international privacy and data protection arena in the past year. The first introduction to this publication in 2013 noted the rapid growth of privacy and data protection laws across the globe and reflected on the commercial and social pressures giving rise to these global developments. Those economic and social pressures have not diminished since that first edition, and they are increasingly triggering new initiatives from legislators to regulate the use of personal information.

The exponential increase of privacy and data protection rules fuels the idea that personal information has become the new 'oil' of today's data-driven economies, with laws governing its use becoming ever more significant.

The same caveat as in previous editions still holds true today: as privacy and data protection rules are constantly evolving, any publication on the topic is likely to be outdated shortly after it is circulated. Therefore, anyone looking at a new project that involves the jurisdictions covered in this publication should verify whether there have been new legislative or regulatory developments since the date of writing.

Convergence of laws

In previous editions of this publication the variation in the types and content of privacy and data protection laws across jurisdictions has been highlighted. It has also been noted that, although privacy and data protection laws in different jurisdictions are far from identical, they often focus on similar principles and common themes.

Policymakers from various parts of the world have been advocating the need for 'convergence' between the different families of laws and international standards since the early days of privacy and data protection law. The thought was that, gradually, the different approaches would begin to coalesce, and that global standards on privacy and data protection would emerge over time. While there is little doubt that convergent approaches to privacy and data protection would benefit both businesses and consumers, it will be a long time before truly global privacy and data protection standards will become a reality.

Privacy and data protection rules are inevitably influenced by legal traditions, cultural and social values, and technological developments which differ from one part of the world to another. Global businesses should take this into consideration, especially if they are looking to introduce or change business processes across regions that involve the processing of personal information (eg, about consumers or employees). Although it makes absolute sense for global businesses to implement common standards for privacy and data protection throughout their organisation, and regardless of where personal information is collected or further processed, there will always be differences in local laws and practices that can have a significant impact on how personal information can or should be used.

International instruments

There are a number of international instruments that continue to have a significant influence on the development of privacy and data protection laws.

The main international instruments are:

- the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108+) of the Council of Europe;
- the OECD Privacy Recommendations and Guidelines (OECD Guidelines);
- the European Union General Data Protection Regulation (GDPR);
- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (the Framework); and
- the African Union Convention on Cyber Security and Personal Data Protection.

Convention 108 was originally adopted in 1981, but was modified in 2018 to more closely reflect data protection norms as they existed at that time. The newly adopted form is known as Convention 108+. Prior to its 2018 update, Convention 108 had been ratified by 53 countries; in June 2018, Cape Verde and Mexico became the fifth and sixth non-European countries, after Mauritius, Uruguay, Senegal and Tunisia, to ratify Convention 108; in 2022, Albania signed the modified Convention 108+, and Armenia and Romania ratified it. As of the date of publication, 46 countries have signed and 17 countries have ratified the modified Convention 108+. Among other things, the modified Convention now includes genetic and biometric data as additional categories of sensitive data, a modernised approach to data subject rights (by recognising a right not to be subjected to automated decision making without the data subject's views being taken into account, and that individuals should be entitled to understand the underlying reasoning behind such processing), and explicitly requires signatories to clearly set forth the available legal bases for processing personal data. Convention 108+ also requires each party to establish an independent authority to ensure compliance with data protection principles and sets out rules on international data transfers. Convention 108+ is open to signature by any country and claims to be the only instrument providing binding standards with the potential to be applied globally. It has arguably become the backbone of data protection laws in Europe and beyond.

The OECD Guidelines are not subject to a formal process of adoption but were put in place by the Council of the OECD in 1980. Like Convention 108, the OECD Guidelines have been reviewed and revisions were agreed in July 2013. Where mostly European countries have acceded to Convention 108, the OECD covers a wider range of countries, including the United States, which has accepted the Guidelines.

Convention 108+ (and its predecessor Convention 108) and the OECD Guidelines originally date from the 1980s. By the 1990s the EU was becoming increasingly concerned about divergences in data protection laws across EU member states and the possibility that intra-EU

trade could be impacted by these divergences. The EU therefore passed Data Protection Directive 95/46/EC, which was implemented by the EU member states with a view to creating an EU-wide framework for harmonising data protection rules. Data Protection Directive 95/46/EC remained the EU's governing instrument for data protection until the GDPR came into force on 25 May 2018.

In 2004, these instruments were joined by a newer international instrument in the form of the APEC Privacy Framework, which was updated in 2015. Although it was subject to criticism when it was launched, the Framework has been influential in advancing the privacy debate in the Asia-Pacific region. The Framework aims to promote a flexible approach to privacy and data protection across the 21 APEC member economies while fostering cross-border flows of personal information. In November 2011, APEC leaders endorsed the Cross-Border Privacy Rules (CBPR) system, which is a voluntary accountability-based system to facilitate privacy-respecting flows of personal information among APEC economies. The APEC CBPR system is considered a counterpart to the European Union's system of binding corporate rules (BCRs) for data transfers outside of the EU. As of the date of publication, nine economies participate in the APEC CBPR system, including the United States, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Taiwan and the Philippines.

In June 2014, the African Union adopted a Convention on Cyber Security and Personal Data Protection as the first legal framework for cybersecurity and personal data protection on the African continent. Its goal is to address the need for harmonised legislation in the area of cybersecurity in member states of the African Union, and to establish in each member state mechanisms to combat privacy violations. To date, the Convention has been signed by 14 African countries and ratified by 13. It has been reported that a number of African countries have drafted data protection laws based on the Convention.

The European approach

For more than 20 years, data protection laws have been a salient feature of European legal systems. Prior to the GDPR, each EU member state introduced legislation based on Data Protection Directive 95/46/EC, which made it mandatory for member states to transpose the Directive's data protection principles into their national laws. In the same way, EU member state rules on electronic communications, marketing and the use of cookies continue to follow the requirements of EU Directive 2002/58/EC on privacy and electronic communications.

Prior to the GDPR, the data protection laws of the EU member states, the European Free Trade Association (Iceland, Liechtenstein and Norway) and EFTA-country Switzerland broadly followed the same pattern, since they were all based on or at least inspired by Data Protection Directive 95/46/EC. However, because Data Protection Directive 95/46/EC was not directly applicable, the laws adopted diverged in many areas. This led to inconsistencies, which created complexity, legal uncertainty and additional costs for businesses that required to comply with, in many cases, 31 different data protection laws in Europe.

This was one of the primary reasons why the European Commission introduced its EU Data Protection Reform in January 2012, which included the GDPR as well as a Data Protection Directive for the police and criminal justice sector (the Police and Criminal Justice Data Protection Directive). The GDPR establishes a single set of rules directly applicable throughout the EU, intended to streamline compliance for companies doing business in the EU. The European Commission estimated that the GDPR could lead to cost savings for businesses of around €2.3 billion a year.

After four years of negotiations, on 15 December 2015 the European Parliament, the Council of the EU and the European Commission reached a compromise on a new and arguably more harmonised data protection framework for the EU. The Council and the Parliament adopted the GDPR (EU 2016/679) and the Police and Criminal Justice Data Protection Directive (EU 2016/680) in April 2016, and the official texts were published the following month. While the GDPR entered into force on 24 May 2016, it became effective on 25 May 2018. The Police and Criminal Justice Data Protection Directive entered into force on 5 May 2016, and EU member states had until 6 May 2018 to transpose it into their national laws.

The GDPR has been a 'game changer' and one of the most significant developments in the history of EU and international data protection law. The impact of the GDPR is not confined to businesses based in the EU, as it applies to any processing of personal information conducted from outside the EU that involves the offering of goods or services to individuals in the EU or the monitoring of individuals in the EU.

As of the date of publication, all EU member states except Slovenia have enacted local data protection laws to supplement the GDPR in a range of areas (eg, sensitive data processing and data processing for employment purposes). However, these legislative initiatives at member state level are not aligned and, therefore, businesses find themselves – once again – in a situation where they have to comply with different member state laws in addition to the GDPR. Furthermore, many data protection authorities in the EU have published their own guidance and recommendations on how to comply with the GDPR, regardless of the guidelines that are being adopted at EU level (by representatives of the EU member state data protection authorities known as the European Data Protection Board or Article 29 Working Party under the previous law). This variety of guidance and recommendations at EU and member state level has triggered confusion for businesses that are trying to determine how to comply with the GDPR.

In April 2016, the European Commission launched a public consultation on the review of the ePrivacy Directive. This review, which intended to pursue consistency between the ePrivacy Directive and the GDPR, raised questions about whether it is still necessary and meaningful to have separate rules on electronic privacy now that the GDPR has been adopted. Following the 2016 consultation, on 10 January 2017 the European Commission adopted a proposal for a Regulation on Privacy and Electronic Communications (the ePrivacy Regulation), which is intended to replace the ePrivacy Directive. The proposal was forwarded simultaneously to the European Parliament, the Council and member state parliaments, as well as to the Committee of the Regions and the Economic and Social Committee for review and adoption. The goal was to have the final text adopted by 25 May 2018, when the GDPR became applicable, but that goal was not achieved. On 10 February 2021, after a number of progress reports and revised drafts of the ePrivacy Regulation, representatives of the EU member states reached an agreement on the Council of the European Union's negotiating mandate for the draft ePrivacy Regulation. The text approved by the EU member states was prepared under Portugal's Presidency and will form the basis of the Council's negotiations with the European Parliament on the final terms of the ePrivacy Regulation. The Council will now begin discussions with the European Parliament to negotiate the final text. Once adopted by the Council and the European Parliament, the draft text provides for a transition period of two years, starting 20 days after the final text of the ePrivacy Regulation is published in the EU Official Journal.

In addition to revamping the legal framework for general data protection, there has been an increased focus on cybersecurity in the EU. Since the adoption of its EU Cybersecurity Strategy in 2013, the European Commission has made laudable efforts to better protect Europeans online, which culminated in an action plan to further strengthen the EU's cyber resilience by establishing a contractual public-private partnership (PPP) with industry in July 2016. In addition, on 6 July 2016, the European Parliament adopted the Network and Information Security (NIS) Directive, which aims to protect 'critical infrastructure' in sectors such as energy, transport, banking and health, as

well as key internet services. Businesses in these critical sectors will have to take additional security measures and notify serious data incidents to the relevant authorities. The NIS Directive entered into force in August 2016, but member states had until May 2018 to transpose the NIS Directive into their national laws. On 25 June 2020, the European Commission launched a public consultation on the revision of the NIS Directive. The European Commission considers a revision to be necessary as cybersecurity capabilities in EU member states remain unequal despite progress made with the NIS Directive, and the level of protection in the EU is insufficient. In addition, the rapid digitalisation of society has expanded the threat landscape and presents new challenges requiring adaptive and innovative responses. On 16 December 2020, a new legislative proposal was presented by the European Commission (NIS 2 Directive), and on 13 May 2022, the European Parliament and the Council of the EU reached a political agreement on the NIS 2 Directive.

In the 2016 referendum, the UK voted to leave the EU. In March 2017, the UK's government formally notified the EU of the UK's referendum decision, triggering Article 50 of the EU's Lisbon Treaty. This signalled the beginning of the process of leaving the EU. The UK left the EU on 31 January 2020 and entered a Brexit transition period that ended on 31 December 2020. Following the end of the transition period, the GDPR no longer applies directly in the UK. In its place, the UK government enacted the Data Protection, Privacy and Electronic Communications (Amendments, etc) Regulations 2019 (EU Exit), which amends the UK Data Protection Act 2018 and merges it with the requirements of the GDPR to form a data protection regime that will work in a UK context after Brexit. This new regime is known as 'the UK GDPR'.

On 19 February 2021, the European Commission published a draft data protection adequacy decision relating to the UK. The draft decision was adopted on 29 June 2021, enabling organisations in the EU to continue to transfer personal data to organisations in the UK without restrictions. In reaching the decision, the European Commission analysed the data protection legal framework in the UK and concluded that the UK's data protection regime meets EU data protection adequacy requirements. The UK has, likewise, recognised the EU as providing an adequate level of protection for personal data. In 2022, the UK government announced its intention to review and modernise the UK's data protection regime, including by diverging from the GDPR in a number of ways to reduce regulatory burdens on business, particularly small businesses. It remains to be seen whether such divergence will lead the EU to continue to recognise the UK as providing an adequate level of protection for personal data.

Global perspective

United States and the EU

Moving outside Europe, the picture is more varied. From an EU perspective, the US is considered to have less regard for the importance of personal information protection. However, the US has had a Privacy Act regulating government departments and agencies since 1974, and there are hundreds of privacy laws at the federal and state level governing various types of information and data processing activities (eg, surveillance laws, biometric data laws and laws requiring online privacy policies). Contrary to the EU's omnibus law approach, the US has historically adopted a sectoral approach to privacy and data protection. For instance, it has implemented specific privacy legislation aimed at protecting children online, the Children's Online Privacy Protection Act 1998 (COPPA). It has also adopted specific privacy rules for health-related data, the Health Insurance Portability and Accountability Act (HIPAA), and for financial institutions, the Gramm-Leach-Bliley Act (GLBA). This approach is beginning to change, with the enactment in California of the nation's first comprehensive privacy, known as the California Consumer Privacy Act of 2018 (CCPA). The CCPA imposes obligations on a range of businesses to provide privacy notices, creates privacy rights of access, deletion and the opportunity to opt out of the sale of personal information, and imposes obligations on businesses to include specified language in their service provider agreements. In November 2020, California voters approved Proposition 24, a ballot referendum to amend the CCPA. Proposition 24, titled the California Privacy Rights Act of 2020 (CPRA), expands certain of the CCPA's compliance obligations and consumer rights. The CPRA will take effect on 1 January 2023. Inspired by California, numerous other states have considered or are actively considering similarly comprehensive privacy legislation. In 2021, two other states, Virginia and Colorado, each enacted comprehensive consumer privacy laws, the Virginia Consumer Data Protection Act and the Colorado Privacy Act, respectively. In 2022, Utah enacted the Utah Consumer Privacy Act, and Connecticut enacted the Connecticut Data Privacy Act. As a result of this state legislative activity, and absent a comprehensive federal privacy and data security law, US businesses are having to contend with a patchwork of different state requirements.

From a cybersecurity perspective, in October 2015, the US Senate passed the Cybersecurity Information Sharing Act (CISA), which aims to facilitate the sharing of information on cyber threats between private companies and US intelligence agencies. A few months later, the US Department of Homeland Security (DHS) issued guidelines and procedures for sharing information under the CISA. The Judicial Redress Act was enacted in February 2016 as a gesture to the EU that the US is taking privacy seriously. The Judicial Redress Act is designed to ensure that all EU citizens have the right to enforce data protection rights in US courts. In May 2017, then-President Trump signed an executive order aimed at strengthening the cybersecurity of federal networks and critical infrastructure.

The US also used to be in a privileged position on account of the EU-US Safe Harbor scheme, which had been recognised by the European Commission as providing adequate protection for the purposes of data transfers from the EU to the US. This formal finding of adequacy for companies that joined and complied with the Safe Harbor was heavily criticised in the EU following the Edward Snowden revelations. On 6 October 2015, in a landmark decision, the Court of Justice of the European Union (CJEU) declared the Safe Harbor invalid. This decision forced thousands of businesses that had relied directly or indirectly on the Safe Harbor to look for alternative ways of transferring personal information from the EU to the US. To address the legal vacuum that was created following the invalidation of the Safe Harbor, the European Commission and the US agreed in February 2016 on a new framework for transatlantic data transfers: the EU-US Privacy Shield.

In accordance with the EU-US Privacy Shield adequacy decision that was adopted in July 2016, the first joint annual review of the Privacy Shield and how it functions in practice took place in September 2017. In its report concluding the first review, the European Commission reiterated its support for the Privacy Shield while outlining certain areas in need of improvement, including the need for ongoing monitoring of compliance with the Privacy Shield Principles by the Department of Commerce and strengthening of the privacy protections contained in the US Foreign Intelligence Surveillance Act (FISA). The Privacy Shield has also been subject to two further joint annual reviews in 2018 and 2019. In the European Commission's report following the latest review, the Commission welcomed further information provided by US authorities in relation to the Foreign Intelligence Surveillance Act and highlighted a number of steps that should be taken to better ensure the effective functioning of the Privacy Shield (eg, by reducing the grace period that applies when organisations are required to recertify annually to a maximum period of 30 days).

Four years after the EU-US Privacy Shield was adopted, the CJEU invalidated the Privacy Shield on 16 July 2020. In a case now known as Schrems II brought by Max Schrems – the privacy activist who is credited with initiating the downfall of Safe Harbor – the CJEU ruled that the

EU-US Privacy Shield was not a valid mechanism to lawfully transfer EU personal data to the US. In the decision, the CJEU held that:

> *the limitations on the protection of personal data arising from [US domestic law] on the access and use [of the transferred data] by U.S. public authorities […] are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary.*

Further, the CJEU found that the EU-US Privacy Shield framework does not grant EU individuals actionable rights before a body offering guarantees that are substantially equivalent to those required under EU law. On those grounds, the CJEU declared the EU-US Privacy Shield invalid. Since the Schrems II decision, US and EU authorities have been negotiating a revised data transfer framework, with those negotiations intensifying in the spring of 2021, as indicated in a 25 March 2021 joint statement by the US Secretary of Commerce, Gina Raimondo, and the European Commissioner for Justice, Didier Reynders. The Biden Administration has stated that establishing a successor agreement to the Privacy Shield is a top priority of the Department of Commerce. On 25 March 2022, the US president and the president of the European Commission announced in a joint statement that the US and the EU have reached an agreement in principle on a new framework to accommodate trans-Atlantic data flows. The framework is expected to be finalised by the end of 2022.

The European Commission recently adopted new Standard Contractual Clauses (new SCCs) in replacement of the existing controller-to-controller and controller-to-processor standard contractual clauses, adopted in 2004 and 2010 respectively. The new SCCs may be used by entities subject to the GDPR to ensure an adequate level of protection for personal data transferred to recipients located in jurisdictions not deemed by the EU to provide an adequate level of protection for personal data transferred, including the US. The new SCCs adopt a modular approach and include provisions that may be used for controller-controller, controller-processor, processor-processor and processor-controller data transfers. While the existing standard contractual clauses have remained a valid data transfer mechanism since the GDPR came into effect, they were drafted under the Data Protection Directive and so do not sit comfortably alongside many of the updates to the EU data protection framework made by the GDPR. The primary purpose of the new SCCs is to provide a data transfer mechanism that operates seamlessly with the legal framework of the GDPR. In addition, following the Schrems II decision, the CJEU held that organisations relying on the standard contractual clauses are required to carry out a case-by-case assessment of whether the standard contractual clauses in fact provide an adequate level of protection, and requires organisations to adduce additional contractual, technical and organisational safeguards where that is not the case. While the new SCCs are unlikely to alleviate such requirements entirely, the new SCCs impose additional obligations on data importers in relation to their handling of government requests for disclosure of or access to EU personal data. At this point in time, the extent to which those provisions are likely to be considered sufficient by EU supervisory authorities remains to be seen. The new SCCs have not been approved for transfers of personal data by organisations located in the UK.

On 2 February 2022, the UK Information Commissioner's Office published an international data transfer agreement (IDTA) and an international data transfer addendum to the European Commission's standard contractual clauses (the Addendum) for use by UK exporters. The IDTA and the Addendum came into force on 21 March 2022.

Asia-Pacific

In the Asia-Pacific region, the early adopters of privacy and data protection laws – Australia, New Zealand and Hong Kong – have been joined by most of the other major jurisdictions. In early 2017, Australia amended its privacy act to introduce data breach notification requirements replacing the previous voluntary regime. New Zealand also amended its privacy law to enact mandatory data breach notification, effective December 2020. China adopted a comprehensive Cybersecurity Law that came into effect on 1 June 2017. China's Cybersecurity Law contains a data localisation requirement applicable to operators of critical information infrastructure. A draft regulation would expand restrictions on cross-border data transfers to all network operators. The law also imposes personal information protection obligations (eg, notice and consent requirements) on network operators, in addition to a data breach notification requirement and obligations to implement cybersecurity protocols. Additional regulations and guidelines also are being considered in relation to the Cybersecurity Law, including draft guidelines concerning the security assessment of cross-border transfers of personal information and important data. Furthermore, on 1 May 2018, the Information Security Technology – Personal Information Security Specification (the Specification) came into effect in China, providing a best practice guide for the processing of personal information. While the Specification is not binding and cannot be used as a direct basis for enforcement, agencies in China can still use the Specification as a reference or guideline in their administration and enforcement activities. In April 2021, China also issued a draft Personal Information Protection Law, marking the introduction of a comprehensive system for the protection of personal information in China; the April 2021 draft was a second version of the bill previously introduced on 21 October 2020 and was issued for public comment.

In April 2018, the Hong Kong Privacy Commissioner for Personal Data announced plans to review and update the 1996 data protection law in light of the GDPR and recent large-scale data breaches affecting Hong Kong citizens' personal data. An additional consultation paper was introduced in January 2020 to propose certain changes to the data protection law, but as of the date of this publication, there is no indication of timeline for amendments to the data protection law.

In December 2016, Indonesia adopted its first data protection law, which focuses on the processing of personal information through electronic media.

Japan amended its Personal Information Protection Act in September 2015, creating an independent data protection authority and imposing restrictions on cross-border data transfers (which took effect in September 2017). On 17 July 2018, the EU and Japan successfully concluded negotiations on a reciprocal finding of an adequate level of data protection, thereby agreeing to recognise each other's data protection systems as 'equivalent'. This will allow personal data to flow legally between the EU and Japan, without being subject to any further safeguards or authorisations. The Personal Data Protection Standard in Malaysia came into force in December 2015 and complements the existing data protection law. In 2017, the Malaysian data protection authority launched a public consultation on the rules regarding cross-border data transfers, which included an initial 'whitelist' of jurisdictions deemed adequate for overseas transfers, but as of the date of this publication, the final whitelist had not been approved. In the Philippines, the implementing rules for the Data Privacy Act of 2012 took effect in September 2016 and the law introduced GDPR-inspired concepts, such as a data protection officer designation and 72-hour breach notification requirements.

Having one of the most advanced data protection regimes in the region, Singapore passed its Cybersecurity Act in February 2018, which provides a national framework for the prevention and management of cyber incidents. In February 2021, Singapore enacted a mandatory data

breach notification law to replace previous non-binding breach notification guidance.

South Korea has lived up to its reputation as having one of the strictest data protection regimes in the Asia-Pacific region. The European Commission is actively engaging with South Korea regarding the possibility of recognising South Korean data protection law as equivalent and hence allowing unrestricted transfers of personal information to South Korea. In Taiwan amendments to the Personal Information Protection Act came into effect in March 2016. The amendments introduced, among other things, rules for processing sensitive personal information. Thailand adopted the Personal Data Protection Act in May 2019, with a one-year grace period until enforcement; however, the implementation deadline subsequently was extended until 1 June 2021.

Finally, in December 2019, the Vietnamese Ministry of Public Security published a six-part draft Decree on Personal Data Protection, which was released for public comments in February 2021. On 8 March 2022, the Vietnamese government issued a resolution on the approval for the dossier of the draft Decree, but further procedural steps are required. As of the time of writing, it is expected that the final decree will likely be adopted in 2022. Vietnam also enacted a Cybersecurity Law in June 2018, but there remains no single comprehensive data protection law in that jurisdiction until the draft Decree enters into force.

Central and South America

Latin America has seen a noticeable increase in legislative initiatives in recent years. Only a handful of Latin American countries currently do not have specific privacy and data protection laws. Argentina and Uruguay have modelled their data protection laws on the EU's approach under the EU Data Protection Directive, which explains why they are the only Latin American countries considered by the European Commission as providing an adequate level of data protection. In February 2017, Argentina initiated a revision process to align its data protection law with the GDPR, introducing concepts such as data portability and 72-hour breach reporting. Chile, Costa Rica, Panama and Peru have launched similar initiatives to Argentina's, while in January 2017 Mexico expanded the scope of its data protection law to cover data processing by private and public persons or entities. Nicaragua passed its data protection law in 2012, but it does not have a fully functioning data protection authority at this point. Other countries in Latin America have some degree of constitutional protection for privacy, including a right to habeas data, for example, in Brazil and Paraguay. On 10 July 2018, Brazil's Federal Senate approved a comprehensive data protection bill, known as the Brazilian General Data Protection Law (LGPD) that was inspired by the GDPR. The LGPD has been in force since August 2021, and a national data protection authority was established in August 2020.

Africa

The global gaps in coverage lie in Africa and the Middle East. However, the number of countries with laws impacting personal information is steadily rising in both regions.

As noted earlier, the African Union adopted a Convention on Cyber Security and Personal Data Protection in June 2014. Initially there were concerns that the Convention was too vague and insufficiently focused on privacy rights. In May 2017, the Commission of the African Union and the Internet Society issued guidelines and recommendations to address these concerns.

An increasing number of African countries are implementing data protection laws as well as cybersecurity regulations irrespective of the Convention–currently, approximately half of the 53 African countries have adopted laws and regulations that relate to the protection of personal data. Angola, for example, introduced its data protection law in 2011 and approved a law in 2016 that would create a data protection authority, although such an authority has not yet been established. Equatorial Guinea's new data protection law entered into force in August 2016 and is clearly inspired by EU data protection standards. Mauritania adopted data protection rules in June 2017, while South Africa passed a data protection law based on the (former) EU model in 2013, which took effect on 1 July 2020. In October 2015, the South African government created a virtual national cybersecurity hub to foster cooperation between the government and private companies. It also introduced a Cybercrimes and Cybersecurity Bill in December 2017, but the Bill was tabled in Parliament. Tanzania passed its Cyber Crime Act in September 2015, and in 2018 Benin updated its earlier 2009 legal framework on data protection, and Uganda is still in the process of preparing the adoption of its first privacy and data protection bill. Four African countries joined Convention 108 between 2016 and 2017: Cape Verde, Mauritius, Senegal and Tunisia. Mauritius also amended its data protection law in light of the EU GDPR, while Morocco published a Q&A in June 2017 and held a seminar in July 2018 on the impact of the GDPR on Moroccan companies. In November 2019, Kenya's comprehensive Data Protection Act entered into force. Most recently, in early 2021, Rwanda approved a comprehensive data protection law.

The Middle East

In the Middle East there are several laws that cover specific industry sectors but, apart from Israel, few countries have comprehensive data protection laws. Israel updated its data protection law in March 2017 by adding data security-related obligations, including data breach notification requirements. The European Commission recognises Israel as a jurisdiction that provides an adequate level of protection of personal data. Qatar passed its first data protection law in November 2016, which is largely inspired by the EU's data protection principles. In January 2018, the Dubai International Financial Centre Authority of the UAE amended its existing data protection law to bring it in line with the GDPR. The UAE's Abu Dhabi Global Market enacted similar amendments to its data protection regulations in February 2018. In July 2020, the Dubai International Financial Centre (DIFC) enacted a replacement for the previous data protection law in that jurisdiction. The new DIFC data protection law took effect on 1 October 2020. The new data protection law was, in part, an effort to help ensure that DIFC, a financial hub for the Middle East, Africa and South Asia, meets the standard of data protection required to receive an 'adequacy' finding from the European Commission and UK to facilitate cross-border transfers of EU and UK personal data to the DIFC without a separate data transfer mechanism. On 2 January 2022, the UAE's first federal Data Protection Law came into force.

Conclusion

Now more than ever, global businesses face the challenge of complying with a myriad of laws and regulations on privacy, data protection and cybersecurity. This can make it difficult to roll out new programmes, technologies and policies with a single, harmonised approach. In some countries, restrictions on cross-border data transfers will apply, while in others localisation requirements may require data to be kept in the country. In some jurisdictions, processing personal information generally requires individuals' consent, while in others consent should be used in exceptional situations only. Some countries have special rules on, for example, employee monitoring. Other countries rely on vague constitutional language to govern data protection.

This publication can hopefully continue to serve as a compass to those doing business globally and help them navigate the (increasingly) murky waters of privacy and data protection.

European Union overview

Aaron P Simpson, David Dumont, James Henderson and Anna Pateraki

Hunton Andrews Kurth LLP

The EU General Data Protection Regulation (GDPR) became directly applicable in all EU member states from 25 May 2018 and in the European Economic Area European Free Trade Association member states (Iceland, Liechtenstein and Norway) in July 2018. The GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) dated 24 October 1995, and established a single set of rules throughout the EU, although EU member state data protection laws complement these rules in certain areas. The EU data protection authorities (DPAs) now gathered in the European Data Protection Board (EDPB) have published a number of guidelines on how to interpret and implement the legal framework. This provides useful guidance to businesses on how to align their data protection practices with the GDPR.

Territorial scope

The GDPR is relevant to both EU businesses and non-EU businesses processing personal data of individuals in the EU. With regard to businesses established in the EU, the GDPR applies to all data processing activities carried out in the context of the activities of their EU establishments, regardless of whether the data processing takes place in or outside of the EU. The GDPR applies to non-EU businesses if they 'target' individuals in the EU by offering them products or services, or if they monitor the behaviour of individuals in the EU.

One-stop shop

One of the most important innovations introduced by the GDPR is the one-stop shop. The GDPR makes it possible for businesses with EU establishments to have their cross-border data protection issues in the EU handled by one DPA acting as a lead DPA. In addition to the lead DPA concept, the GDPR uses the concept of a 'concerned' DPA to ensure that the lead DPA model does not prevent other relevant DPAs from having a say in how a matter is dealt with. The GDPR also sets forth a detailed cooperation and consistency mechanism, in the context of which DPAs exchange information, conduct joint investigations and coordinate enforcement actions. In the case of a disagreement among DPAs with regard to possible enforcement action, the matter can be escalated to the EDPB for a final decision. Purely local complaints without a cross-border element can be handled by the concerned DPA at member state level, provided that the lead DPA has been informed and agrees to the proposed course of action. In some member states, such as France, businesses have to approach the DPA they consider as their lead DPA by filing a specific form for the designation of the lead DPA.

Accountability

Under the GDPR, businesses are held accountable with regard to their data processing operations and compliance obligations, and the GDPR includes a general accountability principle that requires controllers to be able to demonstrate their compliance with the GDPR's obligations. The GDPR also imposes a number of specific obligations on data controllers and data processors in this respect. Data controllers are required to implement and update – where necessary – appropriate technical and organisational measures to ensure that their data processing activities are carried out in compliance with the GDPR, and to document these measures to be able to demonstrate such compliance at any time. This includes the obligation to apply the EU data protection principles at an early stage of product development and by default (privacy by design/default). It also includes the implementation of various compliance tools to be adjusted depending on the risks presented by the data processing activities for the privacy rights of individuals. Data protection impact assessments (DPIAs) are such tools, which have to be conducted in cases of high-risk data processing, and certain other specified processing activities, such as those that involve processing of sensitive data on a large scale. Data processors are required to assist data controllers in ensuring compliance with their accountability obligations, including DPIAs, the implementation of appropriate security measures and the handling of data subject rights requests. In addition, data controllers and data processors have to implement robust data security measures and keep internal records of their data processing activities. Furthermore, in some cases, data controllers and data processors are required to appoint a data protection officer (DPO), for example, if their core activities involve regular and systematic monitoring of individuals or the processing of sensitive data on a large scale. The accountability obligations of the GDPR therefore require businesses to have comprehensive data protection compliance programmes in place.

Data breach notification

The GDPR introduced a general data breach notification requirement applicable to all industries. All data controllers have to notify data breaches to the DPAs without undue delay and, where feasible, within 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Delayed notifications must be accompanied by a reasoned justification, and the information related to the breach can be provided in phases. In addition, data controllers have to notify affected individuals if the breach is likely to result in a high risk to the individuals' rights and freedoms. Businesses must maintain data breach response plans and take other breach readiness measures to avoid fines and the negative publicity associated with data breaches. Data processors are required to notify data controllers of personal data breaches without undue delay after becoming aware of a breach, but do not have an independent obligation to notify DPAs or affected individuals.

Data processing agreements

The GDPR imposes requirements regarding content that must be included in agreements with service providers acting as data processors. The GDPR requires, for example:

- that data processing agreements include documented instructions from the data controller regarding the processing and transfer of personal data to third countries (ie, outside of the EU);

- the processor to implement appropriate data security measures;
- the possibility for the data controller (or a third party mandated by the data controller) to carry out audits and inspections;
- restrictions on the use of sub-processors; and
- an obligation to delete or return personal data to the data controller upon termination of the services.

The EDPB and some DPAs (such as the Danish, French and Spanish DPAs) have developed template clauses to help businesses ensure compliance with those requirements. In June 2021, the European Commission also issued standard contractual clauses that can be used by controllers and processors within the EU and EEA.

Consent

Under the GDPR, consent must be based on a clear affirmative action and be freely given, specific, informed and unambiguous. Consent language hidden in terms and conditions, pre-ticked boxes or inferred from silence is not valid. Also, consent is unlikely to be valid where there is a clear imbalance of power between the individual and the data controller seeking the consent, such as in employment matters. Electronic consent is acceptable, but it has to be clear, concise and not unnecessarily disruptive. In the context of a service, the provision of the service should not be made conditional on customers consenting to the processing of personal data that is not necessary for the service. Further, the GDPR requires data controllers to make additional arrangements to ensure they obtain, maintain and are able to demonstrate valid consent.

Transparency

Under the GDPR, privacy notices must be provided in a concise, transparent, intelligible and easily accessible form to enhance transparency for individuals. In addition to the information that privacy notices already had to include under the previous regime, the GDPR requires that privacy notices specify the contact details of the DPO (if any), the legal basis for the processing, any legitimate interests pursued by the data controller or a third party (where the data controller relies on such interests as a legal basis for the processing), the data controller's data retention practices, how individuals can obtain a copy of the data transfer mechanisms that have been implemented, information about data recipients and whether personal data is used for profiling purposes. When personal data is obtained from a source other than the individual concerned, the data controller must also inform individuals of the source from which the personal data originated and the categories of personal data obtained. In light of the volume of the information required, DPAs recommend adopting a layered approach to the provision of information to individuals (such as the use of a layered privacy notice in a digital context). These transparency requirements require businesses to review their privacy notices regularly.

Rights of individuals

The GDPR strengthens the traditional rights of individuals, such as the rights of access, correction and erasure, and introduces additional rights. For instance, the GDPR strengthens the right of individuals to object to the processing of their personal data. In addition, the GDPR enhances the right to have personal data erased by introducing a 'right to be forgotten'. The right of erasure generally applies when personal data is no longer necessary or, more generally, where the processing of personal data does not comply with or no longer complies with the GDPR; however, it is subject to restrictions. The additional 'right to be forgotten' requires that the data controller communicates a request for erasure of personal data to other data controllers where the data controller has made the personal data public. Furthermore, the GDPR introduces the right to data portability, based on which individuals can request to have their personal data returned to them or transmitted to another data controller in a structured, commonly used and machine-readable format. The right to data portability applies only with regard to automated processing based on consent or processing that is necessary for the performance of a contract. Individuals may also have a right to restrict the processing of personal data in some circumstances, such as when the accuracy of personal data is verified by the data controller. Businesses need to maintain policies and procedures to give effect to the rights of individuals under the GDPR.

Data transfers

The GDPR maintains the general prohibition of data transfers to countries outside of the EU that do not provide an 'adequate' level of data protection, but introduces alternative tools for transferring personal data outside of the EU, such as codes of conduct and certification mechanisms. The previous contractual options for data transfers have been expanded and made easier; regulators may also adopt standard contractual clauses for data transfers to be approved by the European Commission, and it is no longer required to obtain the DPAs' prior authorisation for transferring personal data outside of the EU and submit copies of executed standard contractual clauses (which was previously required in some member states). In addition, the GDPR formally recognises binding corporate rules (BCRs) – internal codes of conduct used by businesses to transfer personal data to group members outside of the EU – as a valid data transfer mechanism for both data controllers and data processors. As a result of the Schrems II decision, the EU-US Privacy Shield Framework is no longer a valid mechanism for transfers of personal data to the US, and organisations that rely on standard contractual clauses (and other transfer mechanisms, such as BCRs) must assess each data transfer on a case-by-case basis to determine whether there is an adequate level of protection for personal data transferred outside the EU and, where necessary, implement additional technical, contractual and organisational safeguards for the transfer. In addition, the European Commission has issued new Standard Contractual Clauses (SCCs) for international data transfers that were adopted on 4 June 2021. Furthermore, the UK Information Commissioner's Office issued an addendum to the EU SCCs and the International Data Transfer Agreement, which were adopted on 2 February 2022.

Administrative fines and right of individuals to effective judicial remedy

In the previous regime, some DPAs (such as the Belgian DPA) did not have the power to impose administrative fines. The GDPR gives this power to all DPAs and introduces high administrative fines that will significantly change the currently fragmented enforcement landscape. Member state DPAs may now impose administrative fines of up to the greater of €10 million or 2 per cent of a company's total worldwide annual turnover, or the greater of €20 million or 4 per cent of a company's total worldwide annual turnover, depending on the nature of the violation. In addition, the GDPR expressly enables individuals to bring proceedings against data controllers and data processors, in particular to obtain compensation for damage suffered as a result of a violation of the GDPR.

The WP29 and EDPB GDPR guidance

The Article 29 Working Party (WP29), composed of representatives of DPAs, has ceased to exist and was replaced by the EDPB as of 25 May 2018. During its first plenary meeting on 25 May 2018, the EDPB endorsed all the GDPR guidelines adopted by the WP29. In total, the WP29 adopted 16 GDPR guidelines and related documents clarifying key concepts and new requirements of the GDPR, including:

- guidelines on the right to data portability;
- guidelines on DPOs;

- guidelines for identifying a data controller or processor's lead DPA;
- guidelines on DPIA and determining whether processing is likely to result in a high risk to the individuals' rights and freedoms;
- guidelines on automated individual decision-making and profiling;
- guidelines on data breach notifications;
- guidelines on administrative fines;
- a BCR referential for data controllers;
- a BCR referential for data processors;
- an adequacy referential;
- guidelines on transparency;
- guidelines on consent;
- an updated working document on BCR approval procedure;
- a revised BCR application form for controller BCRs;
- a revised BCR application form for processor BCRs; and
- a position paper on the derogations from the obligation to maintain internal records of processing activities.

In addition, the EDPB also has adopted guidelines under the GDPR that relate to the following:

- consent under the GDPR;
- the processing of personal data through video devices;
- processing in the context of the provision of online services to data subjects;
- the accreditation of certification bodies under article 43; territorial scope;
- derogations from the prohibition on data transfers;
- the use of location data and contact tracing tools in the context of the covid-19 outbreak;
- the processing of data concerning health for the purpose of scientific research in the context of the covid-19 outbreak;
- criteria of right to be forgotten in search engines;
- concepts of controller and processor in the GDPR;
- data protection by design and by default;
- European Essential Guarantees for surveillance measures; measures that supplement transfer tools;
- the interplay of the Second Payment Services Directive and the GDPR;
- (member state) restrictions under article 23 (national and public security, etc);
- examples regarding data breach notification;
- connected vehicles and mobility related applications;
- virtual voice assistants;
- relevant and reasoned objection under the GDPR;
- certification criteria;
- the application of article 65(1)(a) of the GDPR (ie, dispute resolution);
- the targeting of social media users;
- the legal basis for storage of credit card data for the sole purpose of facilitating further online transactions;
- codes of conduct as tools for transfers;
- the interplay between article 3 (ie, territorial scope) and international data transfers;
- right of access;
- the application of article 60 of the GDPR (ie, cooperation procedure);
- dark patterns in social media platform interfaces;
- the calculation of administrative fines; and
- the use of facial recognition in the area of law enforcement.

EU member state complementing laws

Although the main objective of the GDPR is to harmonise data protection law across the EU, EU member states can and have introduced additional or more specific rules in certain areas; for example, if processing involves health data, genetic data, biometric data, employee data or national identification numbers, or if processing personal data serves archiving, scientific, historical research or statistical purposes. In addition, EU member state laws may require the appointment of a DPO in cases other than those listed in the GDPR. The German Federal Data Protection Act (as revised in 2019), for example, requires businesses to appoint a DPO if they permanently engage at least 20 persons in the data processing, if they carry out data processing activities subject to a DPIA, or if they commercially process personal data for market research purposes. EU member states may also provide for rules regarding the processing of personal data of deceased persons. The French Data Protection Act, as updated on 21 June 2018, for example, includes such rules by granting individuals the right to define the way their personal data will be processed after their death, in addition to the GDPR rights. In the context of online services directed to children, the GDPR requires parental consent for children below the age of 16, but EU member state law may prescribe a lower age limit, provided it is not lower than the age of 13. This limit is lowered to the age of 13, for example, in the Belgian Data Protection Act and the age of 14 in the Austrian Data Protection Amendment Act 2018. At the time of writing, all EU member states other than Slovenia have adopted their new national data protection laws. This creates additional layers of complexity for businesses, which should closely monitor these developments in the relevant member states and assess the territorial scope of the specific national rules, where applicable.

In summary, it is fair to say that the GDPR has created a robust and mature data protection framework in the EU, while EU member state laws complement that framework. The data protection rules affect virtually any business dealing with personal data relating to individuals in the EU. In addition, the GDPR influences data protection laws in different jurisdictions around the world.

The Privacy Shield

Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Twenty-first-century commerce depends on the unencumbered flow of data around the globe. At the same time, however, individuals are clamouring for governments to do more to safeguard their personal data. A prominent outgrowth of this global cacophony has been a reinvigorated regulatory focus on cross-border data transfers. Russia made headlines because it enacted a law in 2015 that requires companies to store the personal data of Russians on servers in Russia. While this is an extreme example of 'data localisation', Russia is not alone in its effort to create impediments to the free flow of data across borders. The Safe Harbor framework, which was a popular tool used to facilitate data flows from the European Union to the United States for nearly 15 years, was invalidated by the Court of Justice of the European Union (CJEU) in 2015, in part as a result of the PRISM scandal that arose in the wake of Edward Snowden's 2013 revelations. The invalidation of Safe Harbor raised challenging questions regarding the future of transatlantic data flows. A successor framework, the EU–US Privacy Shield, was unveiled by the European Commission in February 2016 and in July 2016 was formally approved by the European Union. In 2017, the Swiss government announced its approval of a Swiss–US Privacy Shield framework. Four years after it was formally approved, the EU–US Privacy Shield was invalidated by the CJEU on 16 July 2020, again as a result of concerns arising from the US surveillance framework. The CJEU's decision to invalidate the EU–US Privacy Shield left Shield-certified organisations scrambling to identify and implement alternative data transfer mechanisms to lawfully transfer EU personal data to the United States.

Contrasting approaches to privacy regulation in the European Union and the United States

Privacy regulation tends to differ from country to country, as it represents a culturally bound window into a nation's attitudes about the appropriate use of information, whether by government or private industry. This is certainly true of the approaches to privacy regulation taken in the European Union and the United States, which historically have been both literally and figuratively an ocean apart. Policymakers in the European Union and the United States were able to set aside these differences in 2000 when they created the Safe Harbor framework, which was developed explicitly to bridge the gap between the differing regulatory approaches taken in the European Union and the United States. With the onset of the Privacy Shield, policymakers again sought to bridge the gap between the different regulatory approaches in the European Union and the United States.

The EU approach to data protection regulation

Largely as a result of the role of data accumulation and misuse in the human rights atrocities perpetrated in mid-20th-century Europe, the region has a hard-line approach to data protection. The processing of personal data about individuals in the European Union is strictly regulated on a pan-EU basis by Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR). Unlike its predecessor, Directive 95/46/EC (the Data Protection Directive), the GDPR is not implemented differently at the EU member-state level but applies directly across the European Union.

Extraterritorial considerations are an important component of the data protection regulatory scheme in the European Union, as policymakers have no interest in allowing companies to circumvent EU data protection regulations simply by transferring personal data outside of the European Union. These extraterritorial restrictions are triggered when personal data is exported from the European Union to the vast majority of jurisdictions around the world that have not been deemed adequate by the European Commission; chief among them, from a global commerce perspective, is the United States.

The US approach to privacy regulation

Unlike in the European Union, and for its own cultural and historical reasons, the United States does not maintain a singular, comprehensive data protection law regulating the processing of personal data. Although it is changing with the onset of more comprehensive laws at the state level such as the California Consumer Privacy Act, the California Privacy Rights Act, the Colorado Privacy Act, the Utah Consumer Privacy Act and the Virginia Consumer Data Protection Act, the United States generally favours a sectoral approach to privacy regulation. As a result, in the United States, numerous privacy laws operate at the federal and state levels, and they further differ depending on the industry within the scope of the law. The financial services industry, for example, is regulated by the Gramm-Leach-Bliley Act, while the healthcare industry is regulated by the Health Insurance Portability and Accountability Act of 1996. Issues that fall outside the purview of specific statutes and regulations are subject to general consumer protection regulation at the federal and state level. Making matters more complicated, common law in the United States allows courts to play an important quasi-regulatory role in holding businesses and governments accountable for privacy and data security missteps.

The development of the Privacy Shield framework

As globalisation ensued at an exponential pace during the Internet boom of the 1990s, the differences in the regulatory approaches favoured in the European Union versus the United States became a significant issue for global commerce. Massive data flows between the European Union and the United States were (and continue to be) relied upon by multinationals, and EU data transfer restrictions threatened to halt those transfers. Instead of allowing this to happen, in 2000, the European Commission and the US Department of Commerce joined forces and developed the Safe Harbor framework.

The Safe Harbor framework was an agreement between the European Commission and the US Department of Commerce whereby data transfers from the European Union to the United States made pursuant to the accord were considered adequate under EU law. Previously, to achieve the adequacy protection provided by the framework,

data importers in the United States were required to make specific and actionable public representations regarding the processing of personal data they imported from the European Union. In particular, US importers had to comply with the seven Safe Harbor principles of notice, choice, onward transfer, security, access, integrity and enforcement. Not only did US importers have to comply with these principles, but they also had to publicly certify their compliance with the US Department of Commerce and thus subject themselves to enforcement by the US Federal Trade Commission (FTC) to the extent their certification materially misrepresented any aspect of their processing of personal data imported from the European Union.

From its inception, Safe Harbor was popular with a wide variety of US companies whose operations involved the importing of personal data from the European Union. While many of the companies that certified to the framework in the United States did so to facilitate intracompany transfers of employee and customer data from the European Union to the United States, there are a wide variety of others who certified for different reasons. Many of these include third-party IT vendors whose business operations call for the storage of client data in the United States, including personal data regarding a client's customers and employees. In the years immediately following the inception of the Safe Harbor framework, a company's participation in the Safe Harbor framework, in general, went largely unnoticed outside the privacy community. In the more recent past, however, that relative anonymity changed, as the Safe Harbor framework faced an increasing amount of pressure from critics in the European Union and, ultimately, was invalidated in 2015.

Invalidation of the Safe Harbor framework

Criticism of the Safe Harbor framework from the European Union began in earnest in 2010. In large part, the criticism stemmed from the perception that the Safe Harbor was too permissive of third-party access to personal data in the United States, including access by the US government. The Düsseldorfer Kreises, the group of German state data-protection authorities, first voiced these concerns and issued a resolution in 2010 requiring German exporters of data to the United States through the framework to employ extra precautions when engaging in such data transfers.

After the Düsseldorfer Kreises expressed its concerns, the pressure intensified and spread beyond Germany to the highest levels of government across the Europe Union. This pressure intensified in the wake of the PRISM scandal in the summer of 2013, when Edward Snowden alleged that the US government was secretly obtaining individuals' (including EU residents') electronic communications from numerous online service providers. Following these explosive allegations, regulatory focus in the European Union shifted in part to the Safe Harbor framework, which was blamed in some circles for facilitating the US government's access to personal data exported from the European Union.

As a practical matter, in the summer of 2013, the European Parliament asked the European Commission to examine the Safe Harbor framework closely. In autumn 2013, the European Commission published the results of this investigation, concluding that the framework lacked transparency and calling for its revision. In particular, the European Commission recommended more robust enforcement of the framework in the United States and more clarity regarding US government access to personal data exported from the European Union under the Safe Harbor framework.

In October 2015, Safe Harbor was invalidated by the CJEU in a highly publicised case brought by an Austrian privacy advocate who challenged the Irish Data Protection Commissioner's assertion that the Safe Harbor agreement precludes the Irish agency from stopping the data transfers of a US company certified to the Safe Harbor from Ireland to the United States. In its decision regarding the authority of the Irish Data Protection Commissioner, the CJEU assessed the validity of the Safe Harbor adequacy decision and held it invalid. The CJEU's decision was based, in large part, on the collection of personal data by US government authorities. For example, the CJEU stated that the Safe Harbor framework did not restrict the US government's ability to collect and use personal data or grant individuals sufficient legal remedies when their personal data was collected by the US government.

The Privacy Shield

Following the invalidation of Safe Harbor, the European Commission and US Department of Commerce negotiated and released a successor framework, the EU–US Privacy Shield, in February 2016. Both the EU–US and Swiss–US Privacy Shield frameworks (collectively, the 'Privacy Shield') have since been approved by the European Commission and the Swiss government respectively. The Privacy Shield is similar to Safe Harbor and contains seven privacy principles to which US companies may publicly certify their compliance. Before the invalidation of the EU–US Privacy Shield on 16 July 2020, after certification, entities certified to the Privacy Shield could import personal data from the European Union without the need for another cross-border data transfer mechanism, such as standard contractual clauses. The Swiss–US Privacy Shield similarly permits certified organisations to import personal data from Switzerland without the need for another transfer mechanism. The privacy principles in the Privacy Shield are substantively comparable to those in Safe Harbor but are more robust and more explicit concerning the actions an organisation must take to comply with the principles. In developing the Privacy Shield principles and accompanying framework, policymakers attempted to respond to the shortcomings of the Safe Harbor privacy principles and framework identified by the CJEU.

After releasing the Privacy Shield, some regulators and authorities in the European Union (including the former Article 29 Working Party (WP29), the European Parliament and the European Data Protection Supervisor) criticised certain aspects of the Privacy Shield as not sufficient to protect personal data. For example, the lack of clear rules regarding data retention was heavily criticised. In response to these criticisms, policymakers negotiated revisions to the Privacy Shield framework to address the shortcomings and increase its odds of approval in the European Union. Based on this feedback, the revised Privacy Shield framework was released in July 2016 and formally approved by the European Union. In addition, WP29, which was previously the group of European Union member state data-protection authorities, subsequently offered its support, albeit half-hearted, for the new framework.

First annual review

Under the renegotiated framework, Privacy Shield was subject to annual reviews by the European Commission to ensure it functioned as intended. In September 2017, the US Department of Commerce and the European Commission conducted the first annual joint review of the Privacy Shield, focusing on any perceived weaknesses of the Privacy Shield, including concerning government access requests for national security reasons, and how Privacy Shield-certified entities sought to comply with their Privacy Shield obligations. In November 2017, WP29 adopted an opinion on the review. The opinion noted that WP29 'welcomes the various efforts made by US authorities to set up a comprehensive procedural framework to support the operation of the Privacy Shield'. The opinion also identified some remaining concerns and recommendations concerning both the commercial and national security aspects of the Privacy Shield framework. The opinion indicated that, if the European Union and the United States did not, within specified time frames, adequately address WP29's concerns about the Privacy Shield, WP29 might bring legal action to challenge the Privacy Shield's validity

In March 2018, the US Department of Commerce provided an update summarising actions the agency had taken between January 2017 and March 2018 to support the EU–US and Swiss–US Privacy Shield frameworks. These measures addressed both commercial and national security issues associated with the Privacy Shield. Concerning the Privacy Shield's commercial aspects, the US Department of Commerce highlighted:

- an enhanced certification process, including more rigorous company reviews and reduced opportunities for false claims regarding Privacy Shield certification;
- additional monitoring of companies through expanded compliance reviews and proactive checks for false claims;
- active complaint resolution through the confirmation of a full list of arbitrators to support EU individuals' recourse to arbitration;
- strengthened enforcement through continued oversight by the FTC, which announced three Privacy Shield-related false claims actions in September 2017; and
- expanded outreach and education, including reaffirmation of the framework by federal officials and educational outreach to individuals, businesses and authorities.

Concerning national security, the US Department of Commerce noted measures taken to ensure:

- robust limitations and safeguards, including a reaffirmation by the intelligence community of its commitment to civil liberties, privacy and transparency through the updating and reissuing of Intelligence Community Directive 107;
- independent oversight through the nomination of three individuals to the US Privacy and Civil Liberties Oversight Board (PCLOB) to restore the independent agency to quorum status; individual redress through the creation of the Privacy Shield Ombudsperson mechanism, which provides EU and Swiss individuals with an independent review channel concerning the transfer of their data to the US; and
- US legal developments take into account the Privacy Shield, such as Congress's reauthorisation of section 702 of the Foreign Intelligence Surveillance Act (reauthorising elements on which the European Commission's Privacy Shield adequacy determination was based) and enhanced advisory and oversight functions of the PCLOB.

In June 2018, the debate regarding the Privacy Shield resurfaced when the Civil Liberties Committee of the European Parliament (LIBE) voted on a resolution to recommend that the European Commission suspend the Privacy Shield unless the United States complied fully with the framework by 1 September 2018. This resolution, which passed by a vote of the full European Parliament on 5 July 2018, was a non-binding recommendation. Notwithstanding the result of the full vote, the Privacy Shield was not suspended at that time and continued with the Privacy Shield Principles unchanged.

Second annual review

In October 2018, the US Department of Commerce and the European Commission conducted the second annual review of the Privacy Shield, focusing on all aspects of Privacy Shield functionality. The review found significant growth in the programme since the first annual review and noted several key points, including:

- over 4,000 companies certified to the Privacy Shield since the framework's inception, and the US Department of Commerce's promise to revoke the certification of companies that do not comply with the Privacy Shield's principles;
- the appointment of three new members to the PCLOB by the United States, and the PCLOB's declassification of its report on a presidential directive that extended certain signals intelligence privacy protections to foreign citizens;
- the ongoing review of the Privacy Shield Ombudsperson Mechanism, and the need for the United States to promptly appoint a permanent Under Secretary; and
- recent privacy incidents affecting both US and EU residents reaffirming the 'need for strong privacy enforcement to protect our citizens and ensure trust in the digital economy'.

The European Commission's report on the second annual review (the 2018 Commission Report) of December 2018 furthered several of these points. The 2018 Commission Report concluded that the United States continued to ensure an adequate level of protection to the personal data transferred from the European Union to US companies under the EU–US Privacy Shield. The 2018 Commission Report found that US authorities took measures to implement the European Commission's recommendations from the previous year and several aspects of the functioning of the framework had improved. It also noted, however, several areas of concern, including companies' false claims of participation in and other non-compliance with the Privacy Shield, lack of clarity in Privacy Shield guidance developed by the US Department of Commerce and European Data Protection Authorities, and delayed appointment and uncertain effectiveness of a permanent Privacy Shield Ombudsman.

Subsequently, in January 2019, the European Data Protection Board (EDPB) also issued a report on the second annual review (the 2019 EDPB Report). Although not binding on EU or US authorities, the 2019 EDPB Report guided regulators in both jurisdictions regarding the implementation of the Privacy Shield and highlighted the EDPB's ongoing concerns concerning the Privacy Shield. The 2019 EDPB Report praised certain actions and efforts undertaken by US authorities and the European Commission to implement the Privacy Shield, including for example:

- efforts by the US Department of Commerce to adapt the certification process to minimise inaccurate or false claims of participation in the Privacy Shield;
- enforcement actions and other oversight measures taken by the US Department of Commerce and FTC regarding Privacy Shield compliance; and
- issuance of guidance for EU individuals on exercising their rights under the Privacy Shield, and for US businesses to clarify the requirements of the Privacy Shield.

The 2019 EDPB Report also raised similar concerns regarding:

- the US's ability to oversee and enforce compliance with all Privacy Shield principles (particularly the onward transfer principle);
- delay in the appointment of a permanent Privacy Shield Ombudsman;
- lack of clarity in guidance and conflicting interpretations of various topics, such as the definition of human resource data; and
- shortcomings of the re-certification process, which, according to the 2019 EDPB Report, leads to an outdated listing of Privacy Shield-certified companies and confusion for data subjects.

Third annual review

On 23 October 2019, the European Commission published its report on the third annual review of the Privacy Shield. The report confirmed that the United States continued to provide an adequate level of protection for personal data transferred pursuant to the Privacy Shield and noted several improvements made to the Privacy Shield framework following the second annual review. These improvements included efforts by US authorities to monitor participants' compliance with the Privacy Shield framework and the appointment of Keith Krach, Under Secretary of State for Economic Growth, Energy and the Environment, to the position

of Privacy Shield Ombudsperson on a permanent basis (the vacancy of this position had been flagged in the two previous annual reviews). The European Commission's report on the third annual review noted that the number of Privacy Shield-certified organisations exceeded 5,000 at the time of the report, surpassing the number of companies that had previously registered for the now-defunct Safe Harbor framework in the nearly 15 years that Safe Harbor operated.

In its report on the third annual review, the European Commission also made the following findings and recommendations:

- The European Commission recommended shortening the 'recertification grace period' from the 3.5 months currently permitted by the Department of Commerce to a maximum of 30 days.
- The European Commission also recommended that the Department of Commerce send warning letters to companies who fail to recertify within 30 days of their recertification deadline. The European Commission recommended that the Department of Commerce strengthen its efforts to identify companies that have never certified to the Privacy Shield but nevertheless falsely claim to be certified, noting that the Department of Commerce's verification efforts appear to have been focused on checking whether companies continue to claim Privacy Shield participation even after their certifications had lapsed.
- Concerning enforcement, the European Commission praised the FTC for bringing enforcement actions for violations of the Privacy Shield but recommended that the FTC ensure it can share 'meaningful Information on ongoing investigations' with the European Commission and European data protection authorities.
- The European Commission recommended that data protection authorities continue to refine the definition of what falls within human resources data, given differing interpretations of the term by the various authorities and the lack of clear joint guidance.

Applicability of the Privacy Shield after Brexit

On 20 December 2018, the US Department of Commerce updated its frequently asked questions (FAQs) on the EU–US and Swiss–US Privacy Shield Frameworks to clarify the effect of the United Kingdom's planned withdrawal from the European Union (Brexit). The FAQs, which were updated on 31 January 2020, provided information on the steps Privacy Shield participants would need to take to receive personal data from the United Kingdom in reliance on the Privacy Shield after Brexit. This included requirements for Shield-certified organisations to implement certain changes to their public-facing Privacy Shield representations to expressly state their commitment to apply the Privacy Shield Principles to UK personal data received in the United States in reliance on the Privacy Shield. Pursuant to the Withdrawal Agreement implementing the UK's departure from the European Union, EU law (including EU data protection law) continued to apply in the United Kingdom during the Transition Period of 31 January 2020 to 31 December 2020. During the Transition Period, the European Commission's decision on the adequacy of the protection for personal data provided by the Privacy Shield was to apply to transfers of personal data from the United Kingdom to Privacy Shield participants in the United States. As a result of the end of the Transition Period on 31 December 2020, in these FAQs, the Department of Commerce set a deadline of 31 December 2020 to implement these required changes for the Privacy Shield to serve as a mechanism to transfer UK personal data to the United States lawfully. In addition, the FAQs further stated that if a Privacy Shield participant opted to make such public commitments to continue receiving UK personal data in reliance on the Privacy Shield, the participant would be required to cooperate and comply with the UK Information Commissioner's Office concerning any such personal data received. The FAQs were updated again on 7 June 2021, at which time the Department of Commerce removed the prior FAQs regarding requirements for expressly addressing the UK in public-facing Privacy Shield representations. The updated FAQs indicate that following the UK's exit from the European Union, the UK allows for the transfer of personal data to countries outside the UK only if the transfer is consistent with a UK adequacy decision or is permitted under another applicable safeguard or exception, and that to date, the UK has not adopted an adequacy decision for the US or for the Privacy Shield framework.

Before the UK's exit from the European Union, the United Kingdom adopted regulations that incorporated the GDPR into UK law, taking effect at the end of the Transition Period. The EU–US Privacy Shield was invalidated by the CJEU on 16 July 2020. As of the date of this writing:

- the Privacy Shield is thus no longer a lawful data transfer mechanism concerning UK personal data; and
- the Department of Commerce has not updated its UK-specific FAQs to discuss the impact of the invalidation specifically on the previously released requirements for Shield-certified organisations.

Given the Department of Commerce's stated intention to continue administration and enforcement of the Privacy Shield, to understand their obligations going forward, and until a successor framework is adopted, organisations must keep a careful eye on developments related to the overlapping impacts of the UK's withdrawal from the European Union and the decision to invalidate the Privacy Shield.

US Privacy Shield enforcement actions

The FTC brought numerous enforcement actions against companies for false claims of participation in and non-compliance with the Privacy Shield. In September 2018, the FTC announced settlement agreements with four companies – IDmission, LLC, (IDmission) mResource LLC (doing business as Loop Works, LLC) (mResource), SmartStart Employment Screening, Inc (SmartStart), and VenPath, Inc (VenPath) – over allegations that each company had falsely claimed to have valid certifications under the EU–US Privacy Shield framework. The FTC alleged that SmartStart, VenPath and mResource continued to post statements on their websites about their participation in the Privacy Shield after allowing their certifications to lapse. IDmission had applied for a Privacy Shield certification but never completed the necessary steps to be certified. In addition, the FTC alleged that both VenPath and SmartStart failed to comply with a provision under the Privacy Shield requiring companies that cease participation in the Privacy Shield framework to affirm to the US Department of Commerce that they will continue to apply the Privacy Shield protections to personal information collected while participating in the programme. As part of the FTC settlements, each company is prohibited from misrepresenting its participation in any privacy or data security programme sponsored by the government or any self-regulatory or standard-setting organisation and must comply with FTC reporting requirements. Further, VenPath and SmartStart must either continue to apply the Privacy Shield protections to personal information collected while participating in the Privacy Shield, protect it by another means authorised by the Privacy Shield framework, or return or delete the information within 10 days of the FTC's order.

Similarly, on 14 June 2019, the FTC announced a proposed settlement with a Florida-based background screening company, SecurTest, Inc, over allegations that SecurTest started, but did not complete, an application to certify to the Privacy Shield and nevertheless represented that it was Privacy Shield certified. The proposed settlement would prohibit SecurTest from misrepresenting the extent to which it is a member of any self-regulatory framework, including the Privacy Shield. That same month, the FTC announced it had sent warning letters to 13 US companies for falsely claiming participation in the now-defunct Safe Harbor Framework. In a press release, the FTC stated that it called on the 13 companies to remove from their websites, privacy policies, or any

other public documents any statements claiming participation in Safe Harbor. The FTC noted that it would take legal action if the companies failed to remove such representations within 30 days. Taken together, the recent increase in FTC enforcement of the Privacy Shield demonstrates the agency's commitment to oversee and enforce compliance with the framework's principles.

Between November 2019 and January 2020, the FTC brought an additional 10 enforcement actions against companies alleged to have violated the Privacy Shield by falsely claiming to be certified to the framework. In November 2019, the FTC announced a settlement with Medable, Inc, stemming from allegations that, although Medable did initiate an application with the Department of Commerce in December 2017, the company never completed the steps necessary to participate in the framework. Then, in December 2019, the FTC announced settlements in four separate Privacy Shield cases. Specifically, the FTC alleged that Click Labs, Inc, Incentive Services, Inc, Global Data Vault, LLC, and TDARX, Inc, each falsely claimed to participate in the EU–US Privacy Shield framework. The FTC also alleged that Click Labs and Incentive Services falsely claimed to participate in the Swiss–US Privacy Shield framework and that Global Data and TDARX continued to claim participation in the EU–US Privacy Shield after their Privacy Shield certifications lapsed. The complaints further alleged that Global Data and TDARX failed to comply with the Privacy Shield framework, including by failing to:

- annually verify that statements about their Privacy Shield practices were accurate; and
- affirm that they would continue to apply Privacy Shield protections to personal information collected while participating in the programme.

The following month, in January 2020, the FTC announced five further Privacy Shield settlements. The FTC had alleged, in separate actions, that DCR Workforce, Inc, Thru, Inc, LotaData, Inc, and 214 Technologies, Inc, had made false claims on their websites that they were certified under the EU–US Privacy Shield. In the case of LotaData, the FTC also alleged that the company had falsely claimed certified participation in the Swiss–US Privacy Shield framework. Lastly, the FTC had alleged that EmpiriStat, Inc, falsely claimed current participation in the EU–US Privacy Shield after its certification had lapsed, failed to verify annually that its statements related to its Privacy Shield practices were accurate, and failed to affirm it would continue to apply Privacy Shield protections to personal information it collected while participating in the framework. In each of these cases, as part of the settlements, each of the companies was prohibited from misrepresenting its participation in the Privacy Shield framework, as well as any other privacy or data security programme sponsored by any government, or any self-regulatory or standard-setting organisation.

Following the CJEU's decision to invalidate the EU–US Privacy Shield framework, as described further below, the FTC stated that it continues to expect Shield-certified organisations to comply with their ongoing obligations concerning transfers made previously under the Privacy Shield, including ongoing compliance with the Privacy Shield principles. To that end, following the 16 July 2020 *Schrems II* decision, the FTC announced two Privacy Shield settlements. In October 2020, the FTC announced a settlement with data storage company NTT Global Data Centers Americas, Inc (NTT) in connection with allegations that NTT:

- falsely claimed current participation in the EU–US Privacy Shield after its certification had lapsed; and
- failed to comply with Privacy Shield requirements when participating in the framework.

Notably, when announcing the NTT settlement, the FTC stated that the CJEU's July 2020 decision to invalidate the Privacy Shield framework did not affect the validity of the FTC's decision and order relating to the company's misrepresentations about its participation in and compliance with the Privacy Shield programme. In January 2021, the FTC announced a settlement with fertility app developer Flo Health, Inc over allegations that included violations of the Privacy Shield's notice, choice, accountability for onward transfer, and data integrity and purpose limitation principles, as well as misrepresentations regarding adherence to Privacy Shield principles in the company's privacy policy. As part of these settlements, NTT and Flo Health were prohibited from misrepresenting compliance with or participation in the Privacy Shield framework, as well as any other privacy or data security programme sponsored by any government, or any self-regulatory or standard-setting organisation.

Invalidation of the Privacy Shield framework

On 16 July 2020, the CJEU issued a landmark judgment in a case brought by Max Schrems – the privacy activist who is credited with initiating the downfall of Safe Harbor – deemed *Schrems II*. *Schrems II* was originally heard by Ireland's High Court after Schrems brought a claim against Facebook questioning whether the methods under which technology firms transferred EU citizens' data to the United States afforded EU citizens adequate protection from US surveillance. Specifically, Schrems alleged that the EU Standard Contractual Clauses did not ensure an adequate level of protection for EU data subjects, on the basis that US law does not explicitly limit interference with an individual's right to protection of their personal data in the same way as EU data protection law. Following the complaint, the Irish data protection authority brought proceedings against Facebook in the Irish High Court. In June 2019, the Irish High Court referred the case to the CJEU to determine the legality of the methods used for data transfers through a set of 11 questions referred for a preliminary ruling. The preliminary questions addressed the validity of the Standard Contractual Clauses (SCCs) but also concerned the EU–US Privacy Shield framework.

In *Schrems II*, the CJEU ruled that the EU–US Privacy Shield was not a valid mechanism to lawfully transfer EU personal data to the US. In the decision, the CJEU held that:

> *the limitations on the protection of personal data arising from [US domestic law] on the access and use [of the transferred data] by US public authorities […] are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary.*

Further, the CJEU found that the EU–US Privacy Shield framework does not grant EU individuals actionable rights before a body offering guarantees that are substantially equivalent to those required under EU law. On those grounds, the CJEU declared the EU–US Privacy Shield invalid.

In the aftermath of the *Schrems II* decision, organisations that previously relied on the Privacy Shield to lawfully transfer EU personal data to the United States were required to identify an alternative data transfer mechanism (or applicable derogation under article 49 of the GDPR) to continue transfers of personal data to the US. Following *Schrems II*, companies using SCCs as a transfer mechanism must:

- assess whether the laws in the importing jurisdiction provide an adequate level of protection for personal data transferred under the SCCs; and
- adopt any supplementary measures necessary to ensure adequate protection under EU law.

On 23 July 2020, the EDPB adopted a set of FAQs on the CJEU's decision. These FAQs confirmed that there was no grace period for companies that relied on the EU–US Privacy Shield framework during which they could continue transferring to the United States without assessing the legal basis relied on for those transfers. Transfers based on the EU–US Privacy Shield framework were now, according to the EDPB, illegal. Notably, in November 2020, the European Commission published a draft set of new SCCs that include language regarding the obligation to ensure that data protection laws in the data importer's country do not prevent the importer from complying with the SCCs' requirements, as well as on the data importer's obligations in connection with government access requests, such as notifying the exporter, reviewing the legality of the request and only providing the minimum permissible amount of information under law in response to a request. That same month, the EDPB issued draft recommendations on supplementary measures transferring parties can implement in conjunction with SCCs to help ensure adequate levels of protection following *Schrems II*. In response to the draft SCCs, the US Department of Commerce submitted comments to the European Commission, and the EDPB adopted an opinion providing feedback on the draft clauses. The draft SCCs were finalised on 4 June 2021.

Certain EU data protection authorities also issued statements and guidance in the aftermath of the *Schrems II* decision, taking various stances on the implication of the ruling. For example, the UK Information Commissioner's Office issued a statement that it stood 'ready to support UK organisations . . . to ensure that global data flows may continue and that people's personal data is protected', and subsequently advised organisations to follow the EDPB FAQs on the use of SCCs as 'this guidance still applies to UK controllers and processors'. Certain German data protection authorities took a stronger approach, such as the Berlin data protection commissioner, who called on Berlin-based companies to return EU data currently stored in the United States back to the European Union. In March 2021, the Bavarian data protection authority found the use of email marketing service Mailchimp not to be compliant with *Schrems II* mitigation steps when email addresses were transferred to Mailchimp in the United States. The controller using Mailchimp had relied on SCCs to transfer email addresses to the United States from Germany, but in the Bavarian data protection authority's view, the controller failed to assess the risk of the transfer and implement supplementary measures along with the SCCs. The Bavarian data protection authority did not issue a fine, as the EDPB's draft recommendations on supplementary measures had not yet been finalised, the use of Mailchimp was limited to a small number of instances and the controller cooperated and committed to stop using Mailchimp. Separately, in April 2021, the Portuguese data protection authority highlighted that under *Schrems II*, data protection authorities are obliged to suspend or prohibit data transfers, even when those transfers are based on SCCs, if there are no guarantees that the SCCs can be complied with in the recipient country.

The US Department of Commerce also issued new Privacy Shield FAQs following the *Schrems II* ruling. The new FAQs state that although (as a result of the *Schrems II* ruling) the Privacy Shield:

> *is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States . . . this decision does not relieve participants in the EU–US Privacy Shield of their obligations under the EU–US Privacy Shield Framework*.

The FAQs further state that the Department of Commerce will continue to administer the Privacy Shield programme, including processing applications for self-certification and recertification and maintaining the list of Shield-certified organisations. The FAQs also make clear that organisations that wish to remain on the Privacy Shield list continue to be required to annually recertify to the Privacy Shield framework, including by paying the annual processing fee. As of the date of this writing, the Department of Commerce has taken the view that continued participation in the Privacy Shield 'demonstrates a serious commitment to protect personal information in accordance with a set of privacy principles that offer meaningful privacy protections and recourse for EU individuals'.

Regarding the Swiss–US Privacy Shield, the CJEU decision did not strictly affect the legality of that framework, so the Swiss–US Privacy Shield remained a valid transfer mechanism notwithstanding the ruling. On 16 July 2020, the Federal Data Protection and Information Commissioner of Switzerland (FDPIC) stated that the 'FDPIC has taken note of the CJEU ruling. This ruling is not directly applicable to Switzerland. The FDPIC will examine the judgment in detail and comment on it in due course'. Subsequently, on 8 September 2020, the FDPIC issued an opinion concluding that the Swiss–US Privacy Shield framework does not provide an adequate level of protection for data transfers from Switzerland to the United States under Switzerland's Federal Act on Data Protection. Following this opinion, in practice, companies may no longer rely on the Swiss–US Privacy Shield framework as a valid mechanism for data transfers from Switzerland to the United States. The FDPIC has concluded that organisations must rely on alternative data transfer mechanisms, and must conduct a risk assessment and possibly implement additional safeguards to continue transfers of Swiss personal data to the United States. Nevertheless, the US Department of Commerce has stated that, consistent with its position regarding the impact of the *Schrems II* ruling, the FDPIC opinion does not relieve Swiss–US Shield participants of their obligations under the framework.

Negotiation of a new data transfer framework

In August 2020, the US Department of Commerce and the European Commission announced discussions had been initiated to evaluate the potential for an enhanced EU–US Privacy Shield framework to comply with the CJEU's judgment in *Schrems II*. In March 2021, the US Congressional Research Service released an informational report for members of Congress on EU data transfer requirements and US intelligence laws that summarised potential solutions in the United States to issues raised by *Schrems II*, including:

- an executive order limiting bulk intelligence collection and providing additional redress mechanisms;
- a diplomatic agreement for a new framework to replace the Privacy Shield or a data transfer treaty; and
- legislation that limited bulk intelligence collection or created a cause of action for foreign subjects in the event of unlawful collection.

Later that month, on 25 March 2021, the US Secretary of Commerce, Gina Raimondo, and the European Commissioner for Justice, Didier Reynders, issued a joint statement declaring that the US government and the European Commission had decided to intensify negotiations on an enhanced, alternative data transfer framework to address the judgment of the CJEU in *Schrems II*. The statement noted that 'these negotiations underscore [the parties'] shared commitment to privacy, data protection and the rule of law and [their] mutual recognition of the importance of transatlantic data flows to [their] respective citizens, economies, and societies'. Following this statement, Commissioner Reynders declared in a speech on the digital transatlantic economy that finding a solution on transatlantic data flows 'is a priority in Brussels and in Washington, DC'. For its part, the US Department of Commerce's Privacy Shield press page declared that the 'Privacy Shield and transatlantic data flows are a top priority for the Biden Administration'. In

public comments, EU negotiator Bruno Gencarelli of the European Commission and US negotiator Christopher Hoff of the Department of Commerce each indicated both parties' desire for a 'durable' successor framework.

On 25 March 2022, the president of the European Commission, Ursula von der Leyden, and US President Biden stated in a joint speech that US and EU authorities had agreed, in principle, on a new framework to succeed the Privacy Shield. That same day, the White House issued a fact sheet indicating that the US and the European Commission had committed to a new Trans-Atlantic Data Privacy Framework intended to foster trans-Atlantic data flows and address the CJEU's concerns in *Schrems II*. The fact sheet stated that the framework 'will re-establish an important legal mechanism for transfers of EU personal data to the United States' and that the US:

> *has committed to implement new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives, which will ensure the privacy of EU personal data and to create a new mechanism for EU individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities.*

On 7 April 2022, the EDPB released a statement on the announcement of a new Trans-Atlantic Data Privacy Framework in which the EDPB welcomed the announcement of a political agreement in principle between the European Commission and the US regarding a successor framework to the Privacy Shield. The EDPB indicated that it saw US authorities' commitment to implement measures to protect EU individuals' privacy and personal data as a step in the right direction, but cautioned that the joint announcement did not yet constitute a legal framework that can be relied upon to legitimise transfers between the EU and the US. As of the date of writing, no formal successor framework to the Privacy Shield has been announced or adopted. For the time being, organisations must continue taking necessary measures to comply with the transfer requirements of applicable EU, UK and Swiss law and the *Schrems II* judgment.

Australia

Joshua Annese, Andrea Beatty, Lis Boyce, Andrew Rankin and Craig Subocz*

Piper Alderman

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The legislative framework in Australia is based on both federal laws and state and territory laws.

At the federal level, the collection, use, disclosure and holding of personal information by an agency or organisation to which the Australian Privacy Principles (APPs) apply, including Australian Commonwealth government agencies and most private organisations (excluding small businesses with an annual turnover of less than A$3 million unless they engage in certain activities – see below), is governed by the Privacy Act 1988 (Cth) (the Privacy Act). The Privacy Act incorporates 13 APPs and facilitates additional obligations being imposed on specific sectors by the registration of additional Privacy Codes such as the Credit Reporting Code.

Most Australian states and territories have adopted their own regimes for collecting and handling personal information and for collecting and handling health information that applies to either public sector providers only or both public sector and other health service providers. The state and territory legislative framework is summarised in the table below.

State/territory	Legislation	Applies to
New South Wales	• Privacy and Personal Information Protection Act 1998 (NSW) • The Health Records and Information Privacy Act 2002 (NSW)	Public sector agencies Public sector and other health service providers
Australian Capital Territory	• Information Privacy Act 2014 (ACT) • Health Records (Privacy and Access) Act 1997 (ACT)	Public sector agencies and contracted service providers Public sector and other health service providers
Victoria	• Privacy and Data Protection Act 2014 (Vic) • Health Records Act 2001 (Vic)	Victorian public sector and contracted service providers Public sector and other health service providers
Tasmania	• Personal Information and Protection Act 2004	Public sector agencies
South Australia and Western Australia	No specific privacy legislation	
Northern Territory	• Information Act 2002 (NT)	Public sector agencies
Queensland	• Information Privacy Act 2009 (QLD) • Invasion of Privacy Act 1971 (QLD)	Public sector agencies Any individual or entity

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Privacy Act is administered by the Office of the Australian Information Commissioner.

The Privacy Act grants power to the Information Commissioner to investigate complaints about breaches of the Privacy Act.

As part of an investigation, the Information Commissioner has broad powers to:

- obtain information and documents;
- examine witnesses; and
- issue directions to persons to attend a compulsory conference.

The Information Commissioner also has investigative powers under other statutes, which give the Information Commissioner privacy-related functions, including the power to investigate breaches of the Privacy Safeguards in respect of the Australian Consumer Data Right regime under the Competition and Consumer Act 2010 (Cth).

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Privacy Commissioner is not required to cooperate with data protection authorities overseas. The Commissioner has entered into memorandums of understanding (MOUs) with the Singaporean Personal Data Protection Commissioner, the United Kingdom Information

Commissioner and the Irish Data Protection Commissioner. They outline frameworks between authorities to assist each other with the enforcement of laws protecting PI. They specifically exclude the sharing of PI.

Domestically, the Privacy Commissioner has entered into MOUs with government agencies and regulators such as the Australian Competition and Consumer Commission and the Australian Digital Health Agency to perform specific services in relation to data privacy.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Failing to comply with the Privacy Act may result in proceedings being brought for the imposition of a civil penalty by the Information Commissioner. Some offences under the Privacy Act may lead to criminal prosecution and penalties. The Information Commissioner may also apply for enforceable undertakings and injunctions.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Complainants can:

- seek a merits review of certain decisions by the Administrative Appeals Tribunal under section 96 of the Privacy Act; and
- seek judicial review under the Administrative Decisions (Judicial Review) Act 1977 (Cth) of:
  - an Information Commissioner decision as to whether or not to investigate a complaint; or
  - following an investigation, a determination of the Information Commissioner.

Complainants may also complain to the Commonwealth Ombudsman.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Notwithstanding state and territory-based legislation covering private and public health service providers, the Privacy Act 1988 (Cth) (the Privacy Act) covers all federal government agencies, and all private organisations with an annual turnover of more than A$3 million. The Privacy Act also covers some businesses with a turnover of A$3 million or less, including:

- private sector health providers;
- businesses that purchase personal information;
- credit reporting bodies;
- contracted service providers for Australian government contracts;
- employee associations registered or recognised under the Fair Work (Registered Organisations) Act 2009;
- businesses that hold accreditation under the Consumer Data Right system;
- businesses that have opted in; and
- businesses that are related to a business covered by the Privacy Act.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Privacy Act does not regulate interception of communications or monitoring and surveillance of individuals. It regulates direct marketing (including direct electronic marketing).

The Telecommunications (Interception and Access) Act 1979 (Cth) outlines the general prohibition on intercepting communications passing over telecommunications systems, with exceptions.

The Surveillance Devices Act 2004 (Cth) establishes procedures for law enforcement officers to obtain warrants, emergency authorisations and tracking device authorisations for the installation and use of surveillance devices.

The Spam Act 2003 (Cth) regulates commercial emails and SMS messages by prohibiting their transmission (except with the recipient's consent) and ensuring that any permitted emails and messages contain certain information about the sender and a functional unsubscribe facility.

The Do Not Call Register Act 2006 (Cth) prohibits making unsolicited telemarketing calls or sending unsolicited marketing faxes to numbers on the Do Not Call Register, except with the recipient's consent.

State-based Acts restrict usage of 'surveillance devices', including in the workplace.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

There are several additional laws protecting specific types of data, detailed below.

The My Health Records Act 2012 (Cth) specifies which entities can collect, use and disclose information in the My Health Record system. It also sets out the penalties that can be imposed for improper collection, use and disclosure of such information.

The Australian Prudential Regulation Authority (APRA) regulates authorised deposit-taking institutions in Australia. APRA has established Prudential Standard CPS 234 that requires all APRA-regulated entities to take measures to be resilient against information security incidents. In particular, authorised deposit-taking institutions must take steps to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets.

Thirteen privacy safeguards in Part IVD of the Competition and Consumer Act 2010 (Cth) apply to the handling of personal information collected through Australia's Consumer Data Right regime, largely in substitution of the Australian Privacy Principles. These safeguards set out the privacy rights and obligations for consumers, data holders and accredited data recipients through the regime, including strict requirements in relation to consent.

PI formats

9 | What categories and types of PI are covered by the law?

Personal information under the Privacy Act is information or an opinion about an identified individual or an individual who is reasonably identifiable, regardless of whether the information or opinion is (1) true or (2) recorded in material form.

The above definition is expansive and, as the Full Federal Court made clear in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4, captures all information or opinions about an individual and can include digital and paper records as well as, in some cases, metadata.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Privacy Act has extraterritorial effect provided that the relevant entity has an 'Australian link'. An entity has an Australian link if it is:

- an Australian citizen;
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law;
- a partnership is formed in Australia;
- a trust created in Australia;
- a body corporate incorporated in Australia; or
- an incorporated association with its central management and control in Australia or an external Territory.

However, an organisation also has an Australian link if all of the following apply:

- the organisation is not one of the above;
- the organisation carries on business in Australia; and
- the personal information was collected or held by the organisation in Australia.

In *Facebook Inc v Australian Information Commissioner* [2022] FCAFC 9 (7 February 2022) the court held that it is possible for an entity to carry on business in Australia without a physical presence in Australia, and that Facebook was carrying on business in Australia by installing cookies on devices in Australia and providing Australian application developers with an interface known as the 'Graph API'.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

All collection, use and disclosure of PI is covered by the Privacy Act and generally no distinction is made between those who control or own PI and those who process PI on behalf of the owners. However, generally, where PI is transferred by one person to another person in circumstances where the first person retains control of the PI (eg, where PI is stored on cloud computing infrastructure hosted by another person), the information transfer may constitute a use of the PI by the first party rather than disclosure by the first person and collection by the second person.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

There is no concept of 'legitimate processing' under Australian law. The Australian Privacy Principles specify that an entity may only use, hold or disclose personal information for the primary purpose for which it was collected, or for a secondary purpose if an exception applies. Exceptions include where the individual has consented or they would reasonably expect the entity to use or disclose their personal information for a secondary purpose related to the primary purpose of collection for personal information and in the case of sensitive information, directly related to the primary purpose of collection.

Entities must adopt and make publicly available a privacy policy that sets out how they collect, hold, use and disclose personal information.

Additional restrictions apply under Part IIIA of the Privacy Act in relation to the collection, use, holding and disclosure of credit information and credit reporting information by credit reporting bodies and credit providers, which may only be used and disclosed in specific circumstances. In addition to a general privacy policy, credit reporting bodies and credit providers must also have a credit reporting policy that sets out certain details about the credit information and credit reporting information they collect, hold, use and disclose.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Under the Privacy Act 1988 (Cth), sensitive information is regulated more strictly than other forms of personal information. 'Sensitive Information' is any information or opinion regarding an individual's ethnic or racial origin; political opinions; professional, political or religious affiliations or memberships; sexual orientation or practices; criminal record; health; genetics; and biometrics.

Health information is also subject to additional requirements and restrictions under state and territory legislation. For instance, in New South Wales (NSW), Victoria and the Australian Capital Territory (ACT), health information must only be collected by lawful and fair means. In NSW, health information may only be used for the purpose that it was collected or a directly related purpose, and in the ACT, health information must be collected for a lawful purpose that is directly related to a function or activity of the collector, and the purpose of collection of personal health information must be made known. In Victoria, health information may only be used or disclosed for the primary purpose in which the information was collected or for a directly related and reasonably expected secondary purpose, or if an exception applies.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Owners of personal information must notify individuals about how they use and disclose personal information that they collect. Owners must take reasonable steps to notify individuals at or before the time of collection, or if not practicable, as soon as possible after they collect the person's personal information. The notice must contain information required by the Privacy Act 1988 (Cth) (the Privacy Act):

- the identity and contact details of the entity collecting the information;
- if the entity has collected the information from someone other than the individual or if the individual may not be aware that their personal information has been collected – the fact that the entity has collected the information and the circumstances of that collection;
- if the collection of personal information is required or authorised by law or court order – the fact that the collection is so required or authorised;
- any consequences for the individual if their personal information is not collected by the entity;
- any other entity, body or person to whom the information is usually disclosed by the entity;

- that the entity's privacy policy contains information about how the individual may access their personal information and seek correction of this information;
- that the privacy policy contains information about how the individual can complain about a breach of the Australian Privacy Principles (APPs) or a registered APP code, and how the entity will deal with this complaint; and
- whether the entity is likely to disclose the personal information to overseas recipients, and if so, the countries in which the recipients are likely to be located.

Additionally, at or before the time a credit provider collects personal information it is likely to disclose to a credit reporting body that the credit provider must notify the individual or otherwise ensure the individual is aware of the name and contact details of the credit reporting body and details required to be given to the individual under the Credit Reporting Code and ensure the notice referred to above includes additional information about the credit provider's credit reporting policy and certain rights the individual has under the Privacy Act.

Exemptions from transparency obligations

15 | When is notice not required?

Entities are exempt from the need to comply with the Privacy Act if they engage in certain acts or practices. Exempt entities are not required to notify individuals that their personal information has been collected. The following are exempt:

- individuals in a non-business capacity;
- organisations acting under a Commonwealth contract;
- employee records;
- journalism; and
- organisations acting under a state contract.

Additionally, political acts and practices regarding members of Parliament, contracts for political representatives and volunteers for registered political parties are not subject to the notification requirements.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Entities must take reasonable steps to ensure that the PI collected is accurate, up to date and complete. Furthermore, entities must also take reasonable steps to ensure the information they use or disclose is accurate, up to date, complete and relevant.

PI will be inaccurate if it contains an error or defect, or if it is misleading. An opinion about an individual is not inaccurate by reason that the individual disagrees with the opinion.

PI is incomplete if it presents a partial or misleading picture, rather than a true or full picture.

PI is irrelevant if it does not have a bearing upon or connection to the purpose for which the personal information is used or disclosed.

Whether reasonable steps have been taken will depend on the circumstances, such as the sensitivity of the PI, the nature of the entity's business, the possible adverse consequences for the individual if the quality of the PI is not ensured and the practicability involved.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Government agencies must only collect the personal information reasonably necessary for, or directly related to, one or more of their functions or activities. Private sector organisations must only collect personal information if it is necessary for one or more of their functions or activities.

An agency's functions or activities are conferred by legislation (including subordinate legislation) or an executive scheme or arrangement established by the government. The agency's activities will relate to its functions. These activities include incidental and support activities such as human resources, corporate administration, property management and public relations activities.

The organisation's functions or activities include its current functions or activities, any proposed functions or activities for which the entity has established plans, and activities carried out by the organisation in support of its other functions and activities (such as human resources, corporate administration, property management and public relations activities).

The functions and activities are usually described on a website, in an annual report, in corporate brochures, in advertising, in product disclosure statements and in client and customer letters and emails.

Sensitive information must only be collected if:

- under the first criterion:
  - the individual consents to collection of the information; and
  - if the entity is a government agency, the information is reasonably necessary for, or directly related to, one or more of its functions or activities; or
  - if the entity is a private sector organisation, the information is reasonably necessary for one or more of its functions or activities; and
- under the second criterion;
  - the collection of the information is required or authorised by or under an Australian law or a court or tribunal order;
  - a permitted general situation (eg, lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety) exists in relation to the collection of the information by the entity;
  - the entity is an organisation and a permitted health situation (eg, collection of health information to provide a health service) exists in relation to the collection of the information by the entity;
  - the entity is an enforcement body and the entity reasonably believes that:
    - if the entity is the Immigration Department, the collection of the information is reasonably necessary for, or directly related to, one or more enforcement-related activities conducted by, or on behalf of, the entity; or
    - otherwise, the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or
  - the entity is a non-profit organisation and both of the following apply:
    - the information relates to the organisation's activities of the organisation; and
    - the information relates solely to the organisation's members, or to individuals who have regular contact with the organisation in connection with its activities.

Data retention

18 Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

An entity that holds PI must destroy or de-identify the PI if it no longer needs the information for the purposes for which the information may be used or disclosed. The information must also not be contained in a Commonwealth record.

Entities cannot destroy or de-identify the PI if a law or a court or tribunal orders the entity to retain the information.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Entities may use PI for the primary purpose and any permitted secondary purposes.

The primary purpose is the purpose for which the PI was collected. The secondary purpose is any other purpose other than the primary purpose.

The entity cannot use or disclose information for secondary purposes unless:

- the individual consents to the use or disclosure of information for the secondary purpose; or
- either exception below applies.

If either exception below applies, the entity will be able to use the PI for a secondary purpose.

The first exception applies if:

- the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:
  - directly related to the primary purpose, if the information is sensitive information; or
  - related to the primary purpose, if the information is not sensitive information;
- the use or disclosure of the information is required or authorised by or under an Australian law or a court or tribunal order;
- a permitted general situation exists in relation to the use or disclosure of the information;
- the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or
- the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement-related activities conducted by, or on behalf of, an enforcement body.

The second exception applies if:

- the agency is not an enforcement body;
- the information is biometric information or biometric templates;
- the recipient is an enforcement body; and
- the disclosure is conducted in accordance with the guidelines made by the Information Commissioner.

Specific limitations apply to the use or disclosure of information for direct marketing. Sensitive information collected from an individual should only be used or disclosed for direct marketing to the individual if the individual consents to it. PI (other than sensitive information) can be used to directly market if the individual from whom the information was collected would reasonably expect the information to be used or disclosed for that purpose.

PI (other than sensitive information) can be used for direct marketing if the individual would not reasonably expect the organisation to use or disclose information for that purpose (or the information was collected from a third party), the individual has consented to the use or disclosure of PI for that purpose or it is impracticable to obtain the consent.

In both situations, the organisation must provide a simple means for the individual to opt out of receiving direct marketing communications, and the individual must not have opted out. Additionally, where the recipient would not reasonably expect PI to be used to directly market to them, but has consented to it, the organisation must draw the recipient's attention to the capacity to opt out.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The Privacy Act requires entities to be open and transparent about the purposes for which PI is being collected. If an entity intends to use an individual's PI for making automated decisions without human intervention that affect individuals (including profiling) then this should be noted in the privacy policy. As entities can only use information for a primary or permitted secondary purpose, it is best practice to keep policies and notices updated to ensure that individuals are aware that their PI may be used for automated decision-making purposes, including profiling, if applicable.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Privacy Act 1988 (Cth) (the Privacy Act) requires entities that hold PI to take such steps as are reasonable in the circumstances to protect the information from misuse, interference, loss, and unauthorised access, modification or disclosure. An entity 'holds' personal information if it has possession or control of a record that contains the personal information or it has the right or power to deal with such a record.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The Privacy Act requires entities to notify the Office of the Australian Information Commissioner and affected individuals of 'eligible data breaches' as soon as practicable after confirming the breach. A breach becomes eligible where any unauthorised access to or disclosure of PI held by the entity is likely to result in serious harm to any of the individuals to whom the information relates. If the entity prevents the risk of serious harm to all affected individuals through remedial action, the breach does not need to be notified.

My Health Records

The My Health Records Act 2012 (Cth) requires entities to notify the Australian Information Commissioner of unauthorised collection, use or disclosure of health information included in a My Health Record, or of an event that has (or which may have) occurred that compromises (or which may compromise) the security or integrity of the My Health Record system. The reporting entity must contain the breach, evaluate

the risks arising and arrange for the notification of all healthcare recipients should the entity conclude that the breach is likely to be serious for at least one healthcare recipient.

Prudential Standard CPS 234

Prudential Standard CPS 234 requires entities regulated by the Australian Prudential Regulation Authority (APRA) to notify APRA as soon as possible and no later than 72 hours after becoming aware of an information security incident that materially affects, or has the potential to materially affect (financially or non-financially), the entity or the interests of depositors, policyholders, beneficiaries or other customers, or has been notified to other regulators, either in Australia or other jurisdictions.

Critical infrastructure

The Security of Critical Infrastructure Act 2018 (Cth) requires an entity responsible for critical infrastructure assets to report a cybersecurity incident that has a 'relevant impact' on the asset within 72 hours of becoming aware of the incident and within 12 hours of becoming aware of a 'significant impact'.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Entities must take such steps as are reasonable in the circumstances to:

- protect the PI they hold from misuse, interference and loss and from unauthorised access, modification or disclosure;
- ensure that the PI that the entity collects is accurate, up to date and complete; and
- ensure that the PI that the entity uses or discloses is, with regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There is no requirement to appoint a data protection officer.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

There is no general obligation to maintain internal records relating to PI held by entities. However, the Privacy Act requires entities to make a written note of the use or disclosure of PI based on the entity's reasonable belief that use or disclosure is reasonably necessary for one or more enforcement-related activities.

Credit reporting bodies and credit providers must record, in writing, the use or disclosure of credit information when the information is used in certain contexts, including where the information is used for direct marketing or if the use or disclosure is required by or under an Australian law or a court of tribunal order.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

There is no general obligation for non-government entities to carry out a risk assessment.

Commonwealth government agencies must complete privacy impact assessments (PIAs) for all 'high privacy risk projects' pursuant to the Privacy (Australian Government Agencies – Governance) APP Code 2017.

A PIA must include an initial threshold assessment, a project description, a consultation with stakeholders, a mapping of the information flows, and a privacy impact analysis and compliance check. This check must include:

- the risk of privacy impacts on individuals as a result of how PI is handled;
- whether privacy impacts are necessary;
- whether there are factors that could mitigate negative privacy impacts;
- how the privacy impacts may affect the project's broad goals;
- the project's effect on an individual's choices about who has access to their personal information; and
- compliance with privacy law.

The PIA must outline recommendations to minimise identified risks. Lastly, a PIA process should involve an ongoing process of responding and reviewing changes implemented to minimise risks.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

There is no obligation to apply a privacy-by-design or a by-default approach when designing PI processing systems.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

PI owners or processors are not required to register with the Office of the Australian Information Commissioner (OAIC). However, small businesses and not-for-profit organisations that would otherwise not be captured by the Privacy Act 1988 (Cth) (the Privacy Act), may voluntarily opt in to the Privacy Act and be subject to the Privacy Act. Entities wishing to opt in must complete and submit an application with the OAIC. The Opt-in Register is publicly available on the OAIC's website.

Other transparency duties

29 | Are there any other public transparency duties?

Pursuant to Australian Privacy Principle (APP) 1, entities must manage PI in an open and transparent way. Specifically, entities must have a clearly expressed and up-to-date privacy policy detailing the management of PI by the entity. The privacy policy must specify the types of information collected and held, how the entity collects and holds PI, and the purpose for which PI is collected, held, used and disclosed. The policy must disclose whether the entity will disclose PI to overseas recipients and, if so, the countries in which they are likely to be located. The entity

must take reasonable steps to make its privacy policy available free of charge and in an appropriate form, such as on the entity's website.

APP 5 further requires entities to notify individuals of certain matters at or before the time, or as soon as practicable after, an entity collects PI about an individual, including information regarding the types of PI collected and the purposes for which PI is being collected.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Privacy Act 1988 (Cth) (the Privacy Act) does not use the terms 'processor' or 'service providers', and also does not distinguish between a 'processor' and a 'controller'. Instead, Australian Privacy Principle (APP) 6 outlines the principle governing the use or disclosure of PI generally. APP 6 prohibits use or disclosure of PI for anything other than the primary purpose for which it was collected, unless certain exceptions apply. These exceptions include where the individual consented to the secondary purpose or would have reasonably expected the use or disclosure for the secondary purpose where the secondary purpose is related to the primary purpose.

Where the entity is disclosing the information to a processing organisation that is situated overseas, APP 8, unless an exception applies, creates obligations on the entity to take such steps as are reasonable to ensure that the recipient does not breach the APPs (other than APP 1).

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

There are no direct restrictions on selling personal information or sharing such information for online targeted advertising purposes. Selling and sharing PI for such purposes is controlled by APP 6. APP 6 requires entities to only use or disclose PI for the primary purpose of collection, and any additional, secondary use is only allowed under specific conditions.

Therefore, an entity intending to sell PI must take reasonable steps to notify the individual from whom the information is collected at or before the time of collection (pursuant to APP 5) that the sharing or sale of PI is the entity's primary purpose or, alternatively, be able to justify such a sale as relating to the nominated primary purpose.

The entity to whom the information is sold is likely to be subject to the APPs as a result and needs to comply with the restrictions in APP 7 regarding direct marketing.

The Privacy Act generally exempts businesses with an annual turnover of less than A$3 million from complying with the Privacy Act (including the APPs). However, where an otherwise exempt entity discloses PI about another individual to anyone else for a benefit, service or advantage or provides a benefit, service or advantage to collect PI about another individual from anyone else will make the entity subject to the Privacy Act.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The Privacy Act does not regulate the 'transfer' of PI to overseas third parties as distinct from 'disclosure' of PI to overseas third parties (which is regulated). APP 8.1 provides that disclosure should only occur if the entity takes reasonable steps to ensure that the recipient does not breach the APPs (other than APP 1) in relation to the information. The Office of the Australian Information Commissioner has provided (non-binding) guidance that this generally requires the entity and the overseas recipient to enter into a contract that binds the recipient to comply with the APPs.

APP 8.2 provides that disclosure of PI to an overseas recipient is permitted where:

- the entity reasonably believes that the recipient is subject to laws that have the effect of protecting the information that is substantially equivalent to, or exceeds the protections of, the APPs (and that can be enforced by the individual);
- the individual was informed that if he or she consents, the restriction on overseas disclosure would not apply and he or she consents after being so informed; or
- a 'permitted general situation' exists.

PI is disclosed when an entity makes it accessible to third parties and releases the subsequent handling of the information from its effective control. PI is used when it is handled within the entity's effective control.

Australian organisations that send information overseas under sufficient control and in compliance with the required obligations to constitute transfer may still be held accountable for the overseas organisation mishandling the information, as the Australian organisation still 'holds' the information owing to its degree of control, even if the information is physically located overseas.

Section 16C of the Privacy Act ensures that where an APP entity discloses information to an overseas recipient but the overseas recipient is not subject to the APPs and, where the overseas entity would have breached the APPs (other than APP 1), the APP entity is considered to have undertaken the act and breached the APP instead.

Part IIIA of the Privacy Act imposes restrictions on the disclosure of credit information to overseas recipients. Additionally, state-based privacy laws restrict the transfer of PI (including health information) to recipients located outside the relevant state.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The Privacy Act does not distinguish between first and onward transfers of information overseas. Where information was disclosed to a recipient pursuant to APP 8.1, the information has been disclosed on the basis that the recipient is bound to comply with the APPs in relation to the use and disclosure of the information received from the Australian entity, and the disclosing party may have contractual grounds to enforce such compliance (depending on the terms on which the information was disclosed to the recipient). However, if information has been disclosed to an overseas recipient on the basis of APP 8.2, the Privacy Act would not apply to any onward transfer or disclosure of the information.

Section 16C of the Privacy Act covers the scenario where a disclosure to an overseas entity will not make the overseas entity subject to the APPs under the Privacy Act. In such a scenario, the entity that disclosed the information and is subject to the APPs will be held responsible for any actions of the overseas entity that would have been a breach of the APPs had they applied to the overseas entity.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no general requirement for a copy of PI to be retained in Australia when the PI is transferred overseas.

State laws relating to health records commonly include retention obligations. Where the laws allow the transfer of the health data outside their jurisdiction, such as interstate transfer, there is often a requirement for the record (or information about to whom it was transferred) to be maintained by the original health service provider.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

If an agency or organisation to which the Australian Privacy Principles (APPs) apply holds personal information about an individual, the entity must, on request of the individual, give the individual access to the information. If the entity is an 'agency' (which primarily refers to federal government entities), the agency must respond to a request for personal information within 30 days. If the entity is an 'organisation' (which is defined to include an individual, body corporate, partnership, unincorporated associate or trust), the organisation must respond within a reasonable period after the request is made. While an agency is precluded from charging an individual for requesting or giving access to personal information, organisations may charge individuals for giving access to personal information provided it is not excessive.

If an agency is precluded from disclosing personal information under the Freedom of Information Act or any other Act of the Commonwealth or a Norfolk Island enactment, the agency is not required to comply with a request for information. Notably, an organisation is not required to give an individual access to personal information in a broad number of circumstances including where the request for access is frivolous or vexatious or the organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.

Other rights

36 | Do individuals have other substantive rights?

The Privacy Act 1988 (Cth) (the Privacy Act) provides individuals with a number of protections, including the right to:

- know why personal information is being collected, how it will be used and who it will be disclosed to;
- have the option of using a pseudonym in certain circumstances;
- stop receiving direct marketing;
- have personal information kept accurate, up to date and complete;
- ask for access to personal information (including health information);
- ask for personal information that is incorrect to be corrected; and
- make a complaint to the Office of the Australian Information Commissioner (OAIC) or the relevant external dispute resolution body about an APP entity if it has mishandled personal information.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The Privacy Act makes accommodations for an individual affected by a privacy breach through the dispensation of compensation from the organisation involved in the breach. Where a breach is shown to have occurred, the OAIC may make an order for compensation under section 52 of the Privacy Act. Pursuant to subsection 52(1)(a) or subsection 52(1)(b)(iii), the OAIC may make a declaration that 'the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint'. While there is no monetary ceiling, it is usual that these orders do not exceed the low thousands in Australian dollars. Alternatively, the OAIC may seek orders including injunctions and orders to give a public apology.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

At present, an individual has no exercisable right to make a claim directly against an APP entity for a breach of the Privacy Act. Where an individual has a complaint, their complaint must pass through the OAIC, which may then commence action against the APP entity. The OAIC is empowered with enforcement mechanisms to ensure individuals have access to quick and effective remedies for the protection of their privacy rights. The Privacy Act confers a range of privacy powers on the OAIC to work with entities to facilitate legal compliance and best practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

There is a myriad of exemptions for various entities and their handling of personal information. For example, pursuant to subsection 7B(3) of the Privacy Act 1988 (Cth), a private sector employer's handling of employee records in relation to current and former employment relationships is exempt from the Australian Privacy Principles if the organisation's actions or practices directly relate to:

- a current or former employment relationship between the employer and the individual; or
- an employee record held by the organisation relating to the individual.

Similar exemptions apply to small businesses, registered political parties, political acts and practices, and journalism.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The Privacy Act 1988 (Cth) (the Privacy Act) does not specifically regulate the use of cookies or equivalent technology. However, as cookies and equivalent technology can be used to collect PI, entities must comply with the Australian Privacy Principles (APPs) in relation to the use of cookies (including the disclosure of the use of cookies in privacy policies).

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Privacy Act prohibits APP entities from using or disclosing personal information for the purposes of direct marketing unless certain exemptions apply. In particular, an APP entity can use or disclose PI for the purpose of direct marketing where the PI was collected from the individual and the individual would reasonably expect this use purpose. Direct

marketing is further allowed, where it was not reasonable to expect that the organisation would use the information for direct marketing, but the person gave consent for this use, or obtaining consent was impracticable. This exception applies whether the information was collected from the individual or from a third party. Both exceptions require an easy opt-out mechanism but differ in the degree in which notice of the mechanism must be provided to the individual.

The Spam Act 2003 (Cth) forbids unsolicited commercial electronic messages being sent and requires electronic messages to include an unsubscribe option and information about the individual or the organisation authorising the sending.

The Do Not Call Register Act 2006 (Cth) prohibits businesses from making unsolicited phone calls (eg, telemarketing) or sending unsolicited facsimiles to individuals who have registered their telephone numbers (including mobile phone numbers) or facsimile numbers on the Do Not Call Register, unless specific exceptions apply.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no rules specifically regulating the display of targeted or personalised advertising. Where the information used to target the advertising contains personal information, the entity collecting, holding or disclosing the information will be subject to the Privacy Act (including the APPs).

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

'Sensitive information' is any information or opinion regarding an individual's ethnic or racial origin; political opinions; professional, political or religious affiliations or memberships; sexual orientation or practices; criminal record; health; genetics; and biometrics. This information is under stricter regulation than other forms of personal information under the Privacy Act. Sensitive information may only be collected with consent, except in specified circumstances. Further, sensitive information:

- must not be used or disclosed for a secondary purpose unless the secondary purpose (being within the reasonable expectations of the individual) directly relates to the primary purpose;
- cannot be used for the purposes of direct marketing; and
- cannot be shared between related bodies corporate outside the normal consent and disclosure rules.

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific rules regarding individual profiling. The Privacy Act does not require that an individual is specifically informed of a service using automated processing and profiling, except to the extent that an APP entity is required to disclose the purposes for which PI may be collected as part of general compliance obligations. The Privacy Act does not provide individuals with the right not to be subject to decisions based solely on automated processing, including profiling.

However, the requirements of the Privacy Act may still apply. In particular, APP 6 will protect a user by possibly requiring them to consent where the automated processing and profiling would be part of a purpose that constitutes the secondary rather than primary purpose of collection.

PiperAlderman

Joshua Annese
jannese@piperalderman.com.au

Andrea Beatty
abeatty@piperalderman.com.au

Lis Boyce
lboyce@piperalderman.com.au

Andrew Rankin
arankin@piperalderman.com.au

Craig Subocz
csubocz@piperalderman.com.au

Level 23, Governor Macquarie Tower
1 Farrer Place
Sydney NSW 2000
Australia
Tel: +61 2 9253 9999
www.piperalderman.com.au

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The Office of the Australian Information Commissioner provides guidance explaining that organisations using and sending data to cloud service providers located overseas, under specific conditions, will be considered a 'use' of PI and not a 'disclosure' and will, therefore, be exempt from APP 8.

These conditions include the information being provided for the limited purpose of storing and access by the entity, in addition to creating contractual obligations on the provider that they and any subcontractor may only handle the personal information for these limited purposes. The effective control over how the personal information is handled by the provider must remain with the organisation.

While this use will mean that section 16 and APP 8.1 relating to disclosure will not apply, the cloud service provider will be considered to be 'holding' PI and must comply with APPs 6, 11, 12 and 13.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Over the past year, personal information law has undergone rapid change as advancing technology, social media and cultural values have shifted how industries and individuals perceive their privacy obligations.

In October 2021, the Office of the Australian Information Commissioner released a discussion paper seeking feedback for the ongoing review of the Privacy Act 1988 (Cth) (the Privacy Act) (the Review). In its response to the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry report, the Morrison government committed to undertake a review of the Privacy Act. The Review was commenced on 12 December 2019 and considers whether

the scope of the Privacy Act and its enforcement mechanisms remain fit for purpose. A discussion paper was released in October 2021 and covers a broad range of topics, including:

- the scope and application of the Privacy Act;
- the protections contained in the Australian Privacy Principles (APPs); and
- how the Act is regulated and enforced.

Notably, the discussion paper proposes to introduce a statutory tort for invasions of privacy and create a direct right of action for individuals or groups of individuals whose privacy has been interfered with by an APP entity. Submissions on the discussion paper closed on 10 January 2022, and these contributions will inform the review's final report.

Personal information will continue to adapt and change, as will the policies that regulate it. These aforementioned reforms represent a larger shift towards greater protection of privacy and personal information in Australia in 2022.

* *The authors would like to extend special thanks to Jack Dean, Shannon Hatheier, Jan David Hohmann, Francesca Lombardo and Tom Murdoch for their contributions to the chapter.*

Belgium

David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) became directly applicable in Belgium on 25 May 2018.

In the context of this important evolution of the legal framework, the Belgian data protection supervisory authority (formerly called the Commission for the Protection of Privacy) was reformed by the Act of 3 December 2017 creating the Data Protection Authority (DPA). This reform was necessary to enable the DPA to fulfil the tasks and exercise the powers of a supervisory authority under the GDPR.

On 5 September 2018, the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act) was published in the Belgian Official Gazette. The Data Protection Act addresses the areas where the GDPR leaves room for EU member states to adopt country specific rules and implements Directive (EU) 2016/680 (the Law Enforcement Directive). The Data Protection Act replaced the Act on the Protection of Privacy concerning the Processing of Personal Data of 8 December 1992.

This chapter mainly focuses on the legislative data protection framework for private sector companies and does not address the specific regime for the processing of PI by police and criminal justice authorities in detail. The responses reflect the requirements set forth by the GDPR and the Data Protection Act.

In addition to the GDPR, several international instruments on privacy and data protection apply in Belgium, including:

- Council of Europe Convention 108 on the Protection of Privacy and Trans-border Flows of Personal Data;
- the European Convention on Human Rights and Fundamental Freedoms (article 8 on the right to respect for private and family life); and
- the Charter for Fundamental Rights of the European Union (article 7 on the right to respect for private and family life and article 8 on the right to the protection of personal data).

There is also sector-specific legislation relevant to the protection of PI. The Electronic Communications Act of 13 June 2005 (the Electronic Communications Act), for instance, imposes specific privacy and data protection obligations on electronic communications service providers.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Belgian Data Protection Authority (DPA) is responsible for overseeing compliance with data protection law in Belgium. The DPA is headed by a chair and consists of five main departments, each headed by a director:

- a general secretariat that supports the operations of the DPA and has several executive tasks, including establishing the list of processing activities that require a data protection impact assessment, rendering opinions in the case of prior consultation by a data controller, and approving codes of conduct and certification criteria, as well as standard contractual clauses and binding corporate rules for cross-border data transfers;
- a front office service that is responsible for receiving complaints and requests, starting mediation procedures, raising awareness around data protection with the general public and informing organisations of their data protection obligations;
- a knowledge centre that issues advice on questions related to PI processing and recommendations regarding social, economic or technological developments that may have an impact on PI processing;
- an investigation service that is responsible for investigating data protection law infringements; and
- a litigation chamber that deals with administrative proceedings.

Together, the chairperson and the four directors form the executive committee that, among others, approves the DPA's annual budget and determines the strategy and management plan. The DPA's 2020–2025 Strategic Plan was published on 12 March 2020.

Also, there is an independent reflection board that provides non-binding advice to the DPA on all data-protection-related topics, upon request of the executive committee or the knowledge centre or on its own initiative.

To fulfil its role, the DPA is granted a wide variety of investigative, control and enforcement powers. The enforcement powers include the power to:

- issue a warning or a reprimand;
- order compliance with an individual's requests;
- order to inform affected individuals of a security incident;
- order to freeze or limit processing;
- temporarily or permanently prohibit processing;
- order to bring processing activities in compliance with the law;
- order the rectification, restriction or deletion of PI and the notification thereof to data recipients;
- order the withdrawal of a licence given to a certification body;
- impose penalty payments and administrative sanctions; and
- suspend data transfers.

Further, the DPA can transmit a case to the public prosecutor for criminal investigation and prosecution. The DPA can also publish the decisions it issues on its website. The investigation powers of the DPA include the power to:

- hear witnesses;
- perform identity checks;
- conduct written inquiries;
- conduct on-site inspections;
- access computer systems and copy all data such systems contain;
- access information electronically;
- seize or seal goods, documents and computer systems; and
- request the identification of the subscriber or regular user of an electronic communication service or electronic communication means.

The investigation service also has the power to take interim measures, including suspending, limiting or freezing PI processing activities.

In addition to the DPA, certain public bodies, such as police agencies, intelligence and security services and the Coordination Unit for Threat Analysis, have a specific authority overseeing their data protection compliance.

On 28 January 2022, the Belgian Council of Ministers approved a draft law aimed at reforming the Act of 3 December 2017 creating the DPA. The draft law introduces several changes to the internal structure of the DPA and aims to strengthen parliamentary oversight over the functioning of the DPA. It remains to be seen whether the draft law will be adopted in its current form.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The DPA is required to cooperate with all other Belgian public and private actors involved in the protection of individuals' rights and freedoms, particularly concerning the free flow of PI and customer protection. The DPA must also cooperate with the national data protection authorities of other countries. Such cooperation will focus on, inter alia, the creation of centres of expertise, the exchange of information, mutual assistance for controlling measures and the sharing of human and financial resources. The rules for ensuring a consistent application of the GDPR throughout the European Union outlined in the GDPR will apply in cross-border cases.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The DPA has the power to impose the administrative sanctions outlined in the GDPR. Depending on the nature of the violation, these administrative sanctions can go up to €20 million or 4 per cent of an organisation's total worldwide annual turnover of the preceding financial year. Breaches of data protection law can also lead to criminal penalties, which can, depending on the nature of the violation, go up to €240,000. Also, violations of Belgian privacy and data protection law may result in a civil action for damages.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Decisions of the DPA's Litigation Chamber can be appealed before the Market Court (within the Brussels Court of Appeal) within 30 days of their notification.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Belgian data protection law is generally intended to cover the processing of PI by all types of organisations in all sectors. That said, certain types of PI processing are (partially) exempted or subject to specific rules, including the processing of PI:

- by a natural person in the course of a purely personal or household activity; for example, a private address file or a personal electronic diary;
- solely for journalism purposes, or purposes of academic, artistic or literary expression;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- by the intelligence and security services;
- by the armed forces;
- by competent authorities in the context of security classification, clearances, certificates and advice;
- by the Coordination Unit for Threat Assessment;
- by the Passenger Information Unit; and
- by certain public bodies that monitor the police, intelligence and security services (eg, the Standing Policy Monitoring Committee and the Standing Intelligence Agencies Review Committee).

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act) generally apply to the processing of PI in connection with the interception of communications and electronic marketing, as well as monitoring and surveillance of individuals. Also, these topics are addressed by specific laws and regulations, including:

- the Belgian Criminal Code;
- the Electronic Communications Act of 13 June 2005;
- Collective Bargaining Agreement No. 81 of 26 April 2002 on the monitoring of employees' online communications (interception of communications);
- the Belgian Code of Economic Law;
- the Royal Decree of 4 April 2003 regarding spam (electronic marketing);
- the Belgian Act of 21 March 2007 on surveillance cameras (as amended by the Act of 21 March 2018);
- the Royal Decree of 10 February 2008 regarding the signalling of camera surveillance (as amended by the Royal Decree of 28 May 2018);

- the Royal Decree of 9 March 2014 appointing the categories of individuals authorised to watch real-time images of surveillance cameras in public spaces; and
- Collective Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance in the workplace (surveillance of individuals).

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

A significant number of laws and regulations set forth specific data protection rules that are applicable in a certain area, for example:

- the Act of 21 August 2008 on the establishment and organisation of the e-Health Platform (e-health records);
- Book VII of the Belgian Code of Economic Law on payment and credit services containing data protection rules for the processing of consumer credit data (credit information);
- Collective Bargaining Agreement No. 81 of 26 April 2002 on the monitoring of employees' online communications and the Collective Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance in the workplace;
- the Passenger Data Processing Act of 25 December 2016; and
- the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and the restriction on the use of cash.

PI formats

9 | What categories and types of PI are covered by the law?

The GDPR and the Data Protection Act apply to the processing of PI, wholly or partly by automatic means, and to the processing other than by automatic means of PI that forms part of a filing system (or is intended to form part of a filing system). PI is broadly defined and includes any information relating to an identified or identifiable natural person.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Belgian data protection law applies to the processing of PI carried out in the context of the activities of an establishment of a controller or processor in Belgium. Also, Belgian data protection law can apply to the processing of PI by organisations that are established outside the European Union. This is the case where such organisations process PI of individuals located in Belgium concerning offering goods or services to such individuals in Belgium or monitoring the behaviour of such individuals in Belgian territory.

Belgian data protection law will, however, not apply to the processing of PI by a processor established in Belgium on behalf of a controller established in another EU member state, to the extent that the processing takes place in the territory of the member state where the controller is located. In such a case, the data protection law of the member state where the controller is established will apply.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

In principle, all types of PI processing fall within the ambit of Belgian data protection law, regardless of who is controlling the processing or merely processing PI on behalf of a controller. The controller is any natural or legal person, public authority, agency or other body that alone or jointly with others determines the purposes and means of the processing of PI. Controllers can engage a processor to carry out PI processing activities on their behalf and under their instructions. Controllers are subject to the full spectrum of data protection obligations. Processors, on the other hand, are subject to a more limited set of direct obligations under Belgian data protection law (including the obligation to process PI only on the controller's instructions, keep internal records of PI processing activities, cooperate with the data protection supervisory authorities, implement appropriate information security measures, notify data breaches to the controller, appoint a data protection officer if certain conditions are met and ensure compliance with international data transfer restrictions). In addition to these direct legal obligations, certain data protection obligations will be imposed on processors through their mandatory contract with the controller.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Controllers are required to have a legal basis for each PI processing activity. The exhaustive list of potential legal grounds for the processing of PI outlined in Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) will be available to controllers that are subject to Belgian data protection law:

- the data subject has unambiguously consented to the processing of their PI;
- the processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract;
- the processing is necessary for compliance with a legal obligation under EU or EU member state law to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another individual;
- the processing is necessary for the performance of a task carried out in the public interest or the exercise of the official authority vested in the controller; or
- the processing is necessary for the legitimate interests of the controller (or a third party to whom the PI is disclosed), provided that those interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

For certain types of PI, such as sensitive PI, more restrictive requirements in terms of legal bases apply. Further, controllers that rely on consent to legitimise the processing of PI that takes place in the context of offering information society services to children below the age of 13 years must obtain consent from the child's legal representative.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

The processing of sensitive PI revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data, health data or data concerning a person's sex life or sexual orientation, is only permitted in limited circumstances.

Furthermore, the GDPR prohibits the processing of PI relating to criminal convictions and offences or related security measures, except

where the processing is carried out under the supervision of an official authority or when the processing is authorised by EU or EU member state law. The Data Protection Act allows the processing of PI relating to criminal convictions and offences:

- by natural persons, private or public legal persons for managing their own litigation;
- by lawyers or other legal advisers, to the extent that the processing is necessary for the protection of their clients' interests;
- by other persons, if the processing is necessary to perform duties of substantial public interest that are determined by EU or EU member state law;
- if the processing is required for scientific, historical or statistical research or archiving;
- if the data subject has given their explicit and written consent to the processing of PI relating to criminal convictions and offences for one or more purposes and the processing is limited to such purposes; or
- if the processing concerns PI made public by the data subject, on its own initiative, for one or more specific purposes and the processing is limited to such purposes.

The Data Protection Act also sets forth several specific measures that must be implemented when processing genetic, biometric, health data or PI relating to criminal convictions and offences. In such cases, a list of categories of individuals that will have access to the data, together with a description of those individuals' roles concerning the processing, must be maintained. This list must be made available to the Data Protection Authority upon request. Further, the controller or processor must ensure that the individuals who have access to such data are bound by legal, statutory or contractual confidentiality obligations.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Controllers are required to provide notice to data subjects whose PI they process. If PI is obtained directly from the data subject, the notice must contain at least the following information and be provided no later than the moment the PI is obtained:

- the name and address of the controller (and of its representative, if any);
- the contact details of the data protection officer (if any);
- the purposes of and legal basis for the processing;
- where the legitimate interests' ground is relied upon, the interests in question;
- the existence of the right to object, free of charge, to the intended PI processing for direct marketing purposes;
- the (categories of) recipients of PI;
- details of transfers to third countries or international organisations, the relevant safeguards associated with such transfers (including the existence or absence of an adequacy decision of the European Commission) and how data subjects can obtain a copy of these safeguards or where they have been made available;
- the data retention period or criteria used to determine that period;
- the existence of the right to request access to and rectification or erasure of PI or the restriction of processing of PI or to object to the processing, as well as the right to data portability;
- the existence of the right to withdraw consent at any time if the controller relies on the data subject's consent for the processing of their PI;
- the right to lodge a complaint with a supervisory authority;
- whether providing the PI is a statutory or contractual requirement or a requirement to enter into a contract, as well as whether the data subject is obliged to provide the PI and the possible consequences of the failure to provide the PI; and
- information on automated individual decision-making (if any), including information on the logic involved in such decision-making, the significance and the envisaged consequences.

If PI is not obtained directly from the data subject, the controller must provide, in addition to the information listed above, the categories of PI concerned and the source from which the PI originates. This information must be provided within a reasonable period after obtaining the PI (within one month at the latest), or when PI is shared with a third party, at the very latest when the PI is first disclosed or when the PI is used to communicate with the data subject at the latest at the time of the first communication.

Exemptions from transparency obligations

15 | When is notice not required?

Notice is not required if data subjects have already received the information concerning the processing of their PI required under data protection law.

Also, in cases where PI is not collected directly from the data subject, the controller is exempt from the duty to provide notice if:

- informing the data subject proves impossible or would involve a disproportionate effort, in particular in the context of processing PI for archiving purposes in the public interest, statistical, historical or scientific research, or to the extent that providing notice would seriously impair or render the achievement of the purposes of the processing impossible; or
- PI must remain confidential subject to an obligation of professional secrecy regulated by EU or EU member state law.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Controllers must ensure that the PI they process is accurate and take reasonable steps to ensure that inaccurate PI is rectified or erased without delay.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Controllers are required to limit the processing of PI to what is strictly necessary for processing purposes. In terms of data retention requirements, PI must not be kept in an identifiable form for longer than necessary in light of the purposes for which the PI is collected or further processed. The law imposes stricter conditions for the processing of certain types of PI, such as sensitive data.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Belgian data protection law incorporates the data minimisation and storage limitation principles and, therefore, PI must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and must be kept in a form that permits identification of data subjects for no longer than is necessary for the

purposes for which the PI are processed. This means that PI should be erased or anonymised, as soon as a controller no longer needs the PI in an identifiable form to achieve the purposes for which it was initially collected or further processed.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Belgian data protection law incorporates the 'finality principle' and, therefore, PI can only be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes.

PI can be processed for new purposes if these are not incompatible with the initial purposes for which the PI was collected, taking into account all relevant factors, especially the link between the purposes for which the PI was collected and the purposes of the intended further processing, the context in which the PI was collected, the relationship between the controller and the data subject, the nature of the concerned PI, the possible consequences of the further processing and the safeguards implemented by the controller (eg, pseudonymising or encrypting the PI). Further, the Data Protection Act sets forth specific rules for the further processing of PI for archiving in the public interest, scientific or historical research or statistical purposes.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The use of PI to make automated decisions without human intervention, which produce legal effects or otherwise significantly affect individuals is prohibited unless individuals have consented to it, it is necessary to enter into or perform a contract between the individual and the controller, or it is authorised by EU or EU member state law. Furthermore, additional transparency requirements apply when processing PI for automated decision-making. In such cases, data controllers must provide information about the existence of automated decision-making, the logic involved, and the significance and the envisaged consequences of the decision.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Controllers and processors are required to implement appropriate technical and organisational measures to protect PI from accidental or unauthorised destruction, loss, alteration, disclosure, access and any other unauthorised processing.

These measures must ensure an appropriate level of security considering the condition, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity for the rights and freedoms of individuals.

These measures may include:

- the pseudonymisation and encryption of PI;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to PI promptly in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The more sensitive the PI and the higher the risks for the data subject, the more precautions have to be taken. The Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data, for instance, sets forth specific measures that controllers must implement when processing genetic and biometric data, health data and data relating to criminal convictions and offences, including measures to ensure that persons having access to such PI are under appropriate confidentiality obligations.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The Electronic Communications Act of 13 June 2005 imposes a duty on providers of publicly available electronic communications services to notify security breaches, under certain conditions, to the Data Protection Authority (DPA). The notification should contain the following information:

- the nature of the security breach;
- the consequences of the breach;
- details of the person or persons who can be contacted for more information concerning the breach;
- measures suggested or implemented by the controller to address the breach; and
- measures recommended mitigating the negative effects of the security breach.

Where feasible, the notification should be done within 24 hours after detection of the breach. In case the controller does not have all the required information available within this time frame, it can complete the notification within 72 hours after the initial notification. The DPA has published a template form on its website to accommodate companies in complying with their data breach notification obligations. Also, data subjects must be informed without undue delay when the security breach is likely to adversely affect their privacy or PI.

Since Regulation (EU) 2016/679 (the General Data Protection Regulation) became applicable, mandatory data breach notification obligations are no longer limited to the telecom sector. Controllers in all sectors are now required to notify data breaches to the DPA unless the data breach is unlikely to result in a risk to the rights and freedoms of individuals. Such notification must be done without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. Where notifying the DPA within 72 hours is not possible, the controller must justify such delay. A data breach notification to the DPA must at least contain:

- the nature of the data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of PI records concerned;
- the name and contact details of the data protection officer (if any) or another contact point to obtain additional information regarding the data breach;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken to address the breach, including mitigation measures where appropriate.

In addition to notifying the DPA, controllers are required to notify data breaches to the affected data subjects where the breach is likely to result in a high risk to the rights and freedoms of natural persons. The notification to the affected individuals must contain at least:

- the name and contact details of the data protection officer or another contact person;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken to address the breach, including mitigation measures where appropriate.

Notifying the affected individuals is, however, not required if the controller has implemented measures that render the affected PI unintelligible to any person who is not authorised to access it (eg, encryption), subsequent measures have been taken to ensure that the high risk to the rights and freedoms of individuals is no longer likely to materialise or where notifying the affected individuals would involve a disproportionate effort. In the latter case, public communication or similar measure should be made to inform the affected individuals about the breach. If a processor suffers a data breach, it must notify the controller on whose behalf it processes PI without undue delay. In Belgium, data breaches can be notified to the DPA via an online form made available on the DPA's website.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Belgian data protection law implements the 'principle of accountability', according to which data controllers must implement internal controls to ensure compliance with the law, and to enable them to demonstrate compliance with the law.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The appointment of a data protection officer is mandatory where:

- the processing is carried out by a public authority or body;
- the core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or processor consist of processing sensitive PI on a large scale.

Also, the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act) provides that the appointment of a data protection officer is required for:

- private organisations that process PI on behalf of a public authority (as data processors) or that receive PI from a public authority and the processing of such PI is considered to present a high risk; and
- controllers processing PI for archiving purposes in the public interest or scientific, historical or statistical purposes.

The main tasks of the data protection officer are to:

- inform and advise the controller or processor of its data protection obligations;
- monitor compliance with data protection laws, Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and the controller's or processor's policies, including concerning the assignment of responsibilities, raising awareness and training the controller's or processor's personnel involved in the processing of PI;
- assist with data protection impact assessments;
- cooperate with the relevant supervisory authority; and
- act as a contact point for the data subjects and the relevant supervisory authorities regarding the processing activities, including prior consultation in the context of data protection impact assessments.

Although the obligation to maintain internal records of processing ultimately falls on the controller or processor, the data protection officer may also be assigned the task of maintaining such records.

Controllers and processors must communicate the identity and contact details of their data protection officer to the Data Protection Authority (DPA) via an online form available on the DPA's website.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Controllers and processors are required to maintain internal records of their processing activities. Such records should be in writing, including in electronic form, and should be made available to the DPA upon request.

Controllers' internal records should contain, at least:

- the name and contact details of the controller, joint controller or the controller's representative, if applicable, and the identity and contact details of the data protection officer (if any);
- the purposes of the processing;
- a description of the categories of data subjects and PI;
- the categories of data recipients, including recipients in third countries;
- transfers of PI to a third country, including the identification of such country and, where applicable, documentation of the safeguards that have been put in place to protect the PI transferred;
- the envisaged data retention period or the criteria used to determine the retention period; and
- a description of the technical and organisational security measures put in place, where possible.

Processors' records should contain, at least:

- the name and contact details of the processor and each controller on behalf of which the processor is acting and, where applicable, the controller's or processor's representative and data protection officers;
- the categories of processing carried out on behalf of the controller;
- transfers of PI to third countries, including the identification of such countries and, where applicable, documentation of the safeguards put in place to protect the PI transferred; and
- where possible, a description of the technical and organisational security measures that have been put in place.

Companies that employ fewer than 250 persons are exempted from the obligation to keep internal records of their PI processing activities unless their processing activities are likely to result in a risk to the rights and freedoms of individuals, are not occasional or include the processing of sensitive PI or PI relating to criminal convictions and offences.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

When engaging in new PI processing activities or changing existing processing activities that are likely to result in a high risk to the rights and freedoms of individuals, controllers are also required to carry out a data protection impact assessment. High-risk PI processing activities triggering the requirement to conduct a data protection impact assessment include:

- automated individual decision-making;
- large-scale processing of sensitive PI or PI relating to criminal convictions and offences; and
- systematic monitoring of a publicly accessible area on a large scale.

Where a data protection impact assessment reveals that the PI processing activity would result in a high risk and no measures are taken by the controller to mitigate such risk, the controller must consult the DPA before commencing the envisaged PI processing activity. The Data Protection Act excludes from this requirement, under certain conditions, processing activities for journalistic, academic, artistic or literary purposes.

The DPA issued a Recommendation 01/2018 on data protection impact assessments, in which it provides guidance to controllers on when a data protection impact assessment is required and what the assessment should contain. According to the DPA, a data protection impact assessment must contain a systematic description of the considered PI processing, the purposes of the processing, the PI involved, the categories of recipients and the data retention period, and the material (eg, software, network and papers) on which the PI is saved. The data protection impact assessment must also include an evaluation of the necessity and proportionality of the PI processing activities with regards to the purposes of the processing, taking into account several criteria. Finally, the data protection impact assessment must identify the risks raised by the processing activities and the measures anticipated to address the risks, such as the safeguards, security measures and tools implemented to ensure the protection of the PI and compliance with the GDPR.

Annex 2 of Recommendation 01/2018 includes a list of PI processing activities that require a data protection impact assessment (black list). The list includes, among other things:

- the processing of biometric data for the purpose of uniquely identifying individuals in a public area or private area that is publicly accessible;
- the systematic sharing between several data controllers of special categories of PI or data of a very personal nature (such as data related to poverty, unemployment, youth support or social work, domestic and private activities, and location) between different data controllers;
- collecting health-related data by automated means through an active implantable medical device;
- the processing of PI collected on a large scale by third parties to analyse or predict the economic situation, health, preferences or personal interests, reliability or behaviour, localisation or movements of natural persons; and
- the large-scale processing of PI generated by devices with sensors that send data over the internet or any another means (ie, Internet of Things applications such as smart TVs, smart household appliances, connected toys, smart cities and smart energy systems) for the purpose of analysing or predicting individuals' economic situation, health, preferences or personal interests, reliability or behaviour, localisation or movements.

In addition, Annex 3 of Recommendation 01/2018 includes a list of PI processing activities that do not trigger the requirement to conduct a data protection impact assessment (the white list). The DPA issued a form that should be used in cases where prior consultation with the DPA is required. The form is available on the DPA's website.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The GDPR introduces the principles of privacy by design and privacy by default. Privacy by design means that controllers are required to implement appropriate technical and organisational measures designed to implement the data protection principles effectively and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR. When doing so, controllers must consider the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing. Privacy by default means that controllers must implement appropriate technical and organisational measures to ensure that, by default, only PI that is strictly necessary for each processing purpose is processed.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Since 25 May 2018, the obligation for controllers to register their data processing activities with the Data Protection Authority (DPA) no longer exists. Instead, controllers and processors are required to maintain internal records of their processing activities. However, if a controller or processor appoints a data protection officer, such an appointment must be communicated to the DPA through a specific online form made available on the DPA's website.

Other transparency duties

29 | Are there any other public transparency duties?

No.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Under Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), when a controller outsources data processing activities to a third party (ie, a processor), it should put in place an agreement with the processor that sets out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of PI and categories of data subjects; and
- the obligations and rights of the controller.

Such agreement should stipulate that the processor:

- processes the PI only on documented instructions from the controller, unless otherwise required by EU or EU member state law. In that case, the processor must inform the controller of the legal requirement before processing, unless the law prohibits such

information on important grounds of public interest. Also, if in the processor's opinion an instruction of the controller infringes the GDPR, it should immediately inform the controller thereof;
- ensures that persons authorised to process the PI have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all appropriate technical and organisational measures required under the GDPR to protect the PI;
- shall not engage sub-processors without the specific or general written authorisation of the controller. In the case of a general written authorisation, the processor must inform the controller of intended changes concerning the addition or replacement of sub-processors;
- assists the controller by appropriate technical and organisational measures, insofar as this is possible, with data subjects' rights requests;
- assists the controller in ensuring compliance with the security and data breach notification requirements, as well as the controller's obligation to conduct privacy impact assessments;
- at the end of the provision of the services to the controller, returns or deletes the PI, at the choice of the controller, and deletes existing copies unless further storage is required under EU or EU member state law; and
- makes available to the controller all information necessary to demonstrate compliance with the GDPR and contribute to audits.

On 4 June 2021, the European Commission adopted its new standard contractual clauses to be used between controllers and processors in the European Economic Area. The Controller-Processor standard contractual clauses are aimed at assisting organisations that rely on data processors in the European Economic Area to perform certain data processing activities on their behalf to comply with their obligation to put in place an appropriate data processing agreement, as described above.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

In general, there are no specific restrictions under the GDPR or the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal on the disclosure of PI other than the restrictions resulting from the general data protection principles (such as lawfulness, notice and purpose limitation). Generally, the sharing of PI with a separate data controller that will use the PI for its own marketing purposes requires the data subject's prior consent.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

PI can be transferred freely to other countries within the European Economic Area, as well as to countries recognised by the European Commission as providing an adequate level of data protection.

Transferring PI to countries outside the European Economic Area that are not recognised as providing an adequate level of data protection is prohibited unless:
- the data subject has explicitly given their consent to the proposed transfer after having been informed of the possible risks of such transfers;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject;
- the transfer is necessary for important reasons of public interest or the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or other persons; or
- the transfer is made from a register that is open to consultation either by the public in general or by any person that can demonstrate a legitimate interest.

If none of the above applies and no appropriate safeguards have been put in place, the transfer can take place if it is necessary for compelling legitimate interests pursued by the controller, but only if the transfer is not repetitive, concerns only a limited number of data subjects, and the controller has assessed all circumstances surrounding the data transfer and has provided suitable safeguards to protect the PI. In this case, the controller must inform the Data Protection Authority (DPA) and concerned data subjects of the transfer and the legitimate interests that justify such transfer.

In addition to the exemptions listed above (which should typically only be relied on in limited cases), cross-border transfers to non-adequate countries are allowed if the controller has implemented measures to ensure that the PI receives an adequate level of data protection and data subjects can exercise their rights after the PI has been transferred. Such measures include the execution of standard contractual clauses approved by the European Commission or adopted by a supervisory authority, an approved code of conduct or certification mechanism or implementation of binding corporate rules. When relying on such safeguards to legitimise data transfers, the exporting controller must conduct a transfer risk assessment to verify whether the level of protection for PI transferred is essentially equivalent to the level of protection in the European Union. Depending on the outcome of that assessment, additional safeguards may need to be put in place to ensure such a level of protection for the PI that is transferred. Also, transfers of PI can be legitimised by executing an ad hoc data transfer agreement. However, in such cases, the prior authorisation of the DPA must be obtained.

On 4 June 2021, the European Commission published its implementing decision on standard contractual clauses for the transfer of PI to third countries under the GDPR, along with a set of new standard contractual clauses. The new standard contractual clauses are aimed at replacing the previous version of the clauses that were published by the European Commission in 2001, 2004 and 2010 respectively. The new standard contractual clauses consider the complexity of modern processing chains by combining several general provisions with several modular provisions that should be selected based on the status of the parties under the GDPR, namely provisions for controller-to-controller transfers, controller-to-processor transfers, processor-to-processor transfers and processor-to-controller transfers. The new standard contractual clauses provided for a transition period of three months, during which companies could continue using the old standard contractual clauses. Since 27 September 2021, companies entering into new transfer agreements must use the new standard contractual clauses. Contracts signed before 27 September 2021 that already incorporated the old standard contractual clauses will remain valid until 27 December 2022, provided that the old standard contractual clauses remain unchanged.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The data transfer restrictions and authorisation requirements apply regardless of whether PI is transferred to a service provider (ie, processor) or another controller.

The restrictions and requirements applicable to onward PI transfers depend on the legal regime in the jurisdiction where the data importer is located and the data transfer mechanism relied upon to legitimise the initial data transfer outside the European Economic Area. For example, the standard contractual clauses contain specific requirements for onward data transfers.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no data localisation requirements in Belgium that apply to PI generally. However, certain documents containing PI (such as invoices and other supporting documents related to VAT, company records and companies' social documents) must be kept in Belgium or, when they are stored electronically, full online access from Belgium must be guaranteed.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Data subjects have a right to access the PI that a controller holds about them. When a data subject exercises their right of access, the controller is required to provide the following information to the data subject:

- confirmation as to whether the controller processes the data subject's PI;
- the purposes for which their PI is processed;
- the categories of PI concerned;
- the recipients or categories of recipients to whom PI has been or will be disclosed, in particular, recipients in third countries, and in the case of transfers to third countries, the appropriate safeguards put into place by the controller to legitimise such transfers;
- where possible, the envisaged period for which the PI will be stored or, if not possible, the criteria used to determine such period;
- the existence of the right to request the rectification or erasure of PI or restriction of the processing or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- information regarding the source of the PI; and
- the existence of automated decision-making and information about the logic involved in any such automated decision-making (if any), as well as the significance and the envisaged consequences of such processing.

The controller should also provide a copy of the PI to the data subject in an intelligible form. For further copies requested by the data subjects, controllers may charge a reasonable fee to cover administrative costs.

The right to obtain a copy of PI may be subject to restrictions to the extent it adversely affects the rights and freedoms of others, and the controller may refuse to act on a request of access if the request is manifestly unfounded or excessive, in particular, because of its repetitive character.

Also, exemptions to the right of access apply to PI originating from certain public authorities, including the police and intelligence services and to PI processed for journalistic, academic, artistic or literary purposes.

Other rights

36 | Do individuals have other substantive rights?

Rectification

Data subjects are entitled to obtain, without undue delay, the rectification of inaccurate PI relating to them.

Erasure

Data subjects have the right to request the erasure (the right to be forgotten) of PI concerning them where:

- the PI is no longer necessary for the purposes for which it was collected or otherwise processed;
- the processing is based on consent and the data subject withdraws their consent and there is no other legal basis for the processing;
- the data subject objects to the processing of their PI based on the controller's legitimate interests and there are no overriding legitimate grounds for the processing;
- the data subject objects to the processing of their PI for direct marketing purposes;
- PI has been unlawfully processed;
- PI has to be erased for compliance with a legal obligation under EU or EU member state law; and
- PI has been collected concerning offering information society services to a child.

The right to be forgotten does not apply where the processing is necessary for:

- the exercise of the right to freedom of expression and information;
- compliance with a legal obligation under EU or EU member state law;
- the performance of a task carried out in the public interest or the exercise of official authority vested in the controller;
- reasons of public interest in the area of public health;
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- the establishment, exercise or defence of legal claims.

Restriction of processing

Data subjects are entitled to request that the processing of their PI is restricted by the controller, where one of the following conditions applies:

- the data subject is contesting the accuracy of their PI, in which case, the processing should be restricted for a period enabling the verification by the controller of the accuracy of the PI;
- the processing is unlawful and the data subject opposes the erasure of the PI and requests the restriction of its use instead;
- the controller no longer needs the PI, but the PI is required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to the processing of their PI for purposes other than direct marketing, based on grounds relating to their particular situation. In this case, the processing should be restricted, pending the verification by the controller as to whether the controller's legitimate interests override those of the data subject.

Objection to processing

Data subjects have the right to object at any time to the processing of their PI for substantial and legitimate reasons related to their particular situation, where the 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 where the controller processes the PI to pursue its legitimate interests. Also, data subjects are in any event (ie, without any specific justification) entitled to object, at any time, to the processing of their PI for direct marketing purposes.

Data portability

Data subjects are entitled to receive in a structured, commonly used and machine-readable format the PI they have provided directly to the controller and the PI they have provided indirectly by the use of the controller's services, websites or applications. Also, where technically feasible, data subjects have the right to have their PI transmitted by the controller to another controller. The right to data portability only applies if:

- the PI is processed based on the data subject's consent or the necessity of the processing for the performance of a contract; and
- the PI is processed by automated means.

The above-mentioned rights are subject to certain restrictions, in particular in the case of processing PI originating from certain public authorities, including the police and intelligence services, or processing of PI for journalistic, academic, artistic or literary purposes.

Complaint to relevant supervisory authorities and enforce rights in court

Data subjects are entitled to file a complaint with the DPA (which has been granted investigative, control and enforcement powers) to enforce their rights. Further, data subjects can initiate proceedings before the President of the Court of First Instance when their rights have not been respected by the controller.

Automated decision-making

Data subjects also have the right not to be subject to decisions having legal effects or significantly affecting them, including profiling, which are taken purely based on automatic data processing, unless the decision:

- is necessary to enter into or for the performance of a contract;
- is based on a legal provision under EU or EU member state law; or
- is based on the data subject's explicit consent.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Data subjects are entitled to receive compensation from controllers if they have suffered material or non-material damages as a result of a violation of Belgian data protection law. Controllers will only be exempt from liability if they can prove that they are not responsible for the event giving rise to the damage. Individuals may choose to mandate an organ, organisation or non-profit organisation to lodge a complaint on their behalf before the Data Protection Authority (DPA) or the competent judicial body.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Enforcement of data subjects' rights is possible through legal action before the Belgian courts (ie, before the President of the Court of First Instance) and via the DPA.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

No.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Cookies or any other type of information can only be stored or accessed on individuals' equipment provided that the individuals have consented after having been informed about the use of such cookies. However, individuals' opt-in consent is not required if the access to or storage of information on their equipment is for the sole purpose of carrying out the transmission of a communication over an electronic communications network or is strictly necessary to provide a service explicitly requested by the individual.

On 9 April 2020, the Data Protection Authority (DPA) updated its practical guidance on cookies intending to clarify how companies should inform individuals about and obtain their consent for the use of cookies, as well as the types of cookies that are exempted from the consent requirement.

The guidance provides that consent must be informed, unambiguous and provided through a clear affirmative action. Merely continuing to browse a website does not constitute valid consent. Users must have the possibility to provide granular consent per type of cookie, as well as, in a second stage, per cookie. Also, users must be provided with information regarding the use of cookies. The DPA suggests providing this information in two phases: first, a notice at the time the users' consent is obtained, and second, a more detailed notice in the form of a cookie policy.

According to the DPA, users must be provided with the following information upon consenting to the use of cookies:

- the entity responsible for the use of cookies;
- the purposes for which cookies are used;
- the data collected through the use of cookies;
- the cookies' expiry time; and
- the users' rights concerning cookies, including the right to withdraw their consent.

The DPA also clarifies that the lifespan of a cookie must be limited to what is necessary to achieve the cookie's purpose and cookies should not have an unlimited lifespan.

The cookie requirements under Belgian law result from the legal regime for the use of cookies set forth by Directive 2002/58/EC (the ePrivacy Directive), as transposed into EU member state law. The ePrivacy Directive is currently under review and will most likely be replaced by the ePrivacy Regulation in the future. The exact timing of the adoption of the ePrivacy Regulation has, however, not yet been determined.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Apart from the general rules on marketing practices and specific rules on marketing for certain products or services (eg, medicines and financial services), there are specific rules for marketing by email, fax and telephone.

Marketing by electronic post

Sending marketing messages by electronic post (eg, email or text) is only allowed with the prior, specific, free and informed consent of the addressee. However, provided that certain conditions are fulfilled, electronic marketing to legal persons and existing customers is exempt from the opt-in consent requirement. In any event, electronic marketing messages should inform the addressee about their right to opt-out from receiving future electronic marketing and provide appropriate means to exercise this right electronically. Also to the consent requirement, Belgian law sets out specific requirements concerning the content of electronic marketing messages, such as the requirement that electronic marketing should be easily recognisable as such and should clearly identify the person on whose behalf it is sent.

Marketing by automated calling systems and fax

Direct marketing by automated calling systems (without human intervention) and fax also requires the addressees' prior, specific, free and informed consent. Further, the addressee should be able to withdraw their consent at any time, free of charge and without any justification.

Marketing by telephone

Belgian law explicitly prohibits direct marketing by telephone to individuals who have registered their telephone number with the Do Not Call register.

As the rules on electronic communications marketing under Belgian law result from the ePrivacy Directive, these rules may change once the ePrivacy Directive is replaced by the ePrivacy Regulation (which has not been adopted yet). Also, on 10 February 2020, the DPA published Recommendation 1/2020 on data processing activities for direct marketing purposes, which aims at clarifying the complex rules relating to the processing of PI for direct marketing purposes and provides practical examples and guidelines around direct marketing.

Among others, Recommendation 1/2020 clarifies that:

- Determining and specifying the purposes for which PI will be processed is essential. In this respect, the DPA considers that merely stating that personal data will be processed for direct marketing purposes is not sufficient in light of the transparency requirements applicable under Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR).
- To ensure data minimisation, companies should limit open fields in data collection forms, review their databases regularly to delete any unnecessary data, and implement processes to ensure that Do Not Call lists are considered when reviewing databases where marketing data is stored.
- Individuals must be offered a right to object at any time and easily, without having to take additional steps and free of charge, to the processing of their PI for direct marketing purposes. In this respect, the DPA considers that a simple unsubscribe button in small characters at the end of a marketing email is not sufficient. Also, where it is technically feasible, the DPA recommends allowing individuals to granularly select the marketing activities for which they want to object (eg, email marketing or text).
- Consent to direct marketing must be specific concerning the content of the marketing communication and the means used.
- Where an individual withdraws their consent to the processing of PI, there is no longer a valid legal ground unless PI must be kept to comply with a legal obligation. In practice, this means that if the individual withdraws their consent and there is no alternative legal ground, PI should be deleted (regardless of whether the individual exercises their deletion rights). The same applies where individuals object to the processing of their PI based on the legitimate interest ground.

Targeted advertising

42 | Are there any rules on targeted online advertising?

Online targeted advertising, such as through the use of cookies, requires individuals' prior opt-in consent.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The processing of sensitive PI revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data, health data or data concerning a person's sex life or sexual orientation, is prohibited in principle, and can only be carried out if:

- the data subject has given their explicit consent to such processing;
- the processing is necessary to carry out the specific obligations and rights of the controller or the data subject in the employment, social security or social protection law area;
- the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving their consent;
- the processing is carried out by a foundation, association or any other non-profit organisation with political, philosophical, religious or trade union objectives in the course of its legitimate activities, and solely relates to the member or former members of the organisation or to persons that have regular contact with the organisation and the PI is not disclosed to third parties without the data subject's consent;
- the processing relates to PI that has been manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for reasons of substantial public interest recognised by EU or EU member state law;
- the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services based on EU or EU member state law or according to a contract with a health professional, subject to appropriate confidentiality obligations;
- the processing is necessary for reasons of public interest in the area of public health based on EU or EU member state law; or
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EU or EU member state law.

The Data Protection Act explicitly lists several PI processing activities that (provided certain conditions are met) can be deemed as necessary for reasons of substantial public interest, including PI processing activities of human rights organisations, the Centre for Missing and Sexually Exploited Children (Child Focus), and organisations that assist sex offenders.

Profiling

44 | Are there any rules regarding individual profiling?

Profiling that does not produce legal effects on individuals or does not significantly affect them is generally not subject to specific rules and can be legitimised using several potential legal bases, including the legitimate interests legal basis, provided that individuals are clearly informed about the controller's profiling activities, taking into account the transparency requirements of the GDPR.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There are no specific rules on the use of cloud computing services under Belgian law. However, the DPA has issued advice (Advice No. 10/2016 of 24 February 2016 on the Use of Cloud Computing by Data Controllers) that identifies the privacy risks related to cloud computing services and provides guidelines for data controllers on how to comply with Belgian data protection law when relying on providers of cloud computing services.

Some of the risks identified by the DPA include:

- loss of control over the data owing to physical fragmentation;
- increased risk of access by foreign authorities;
- vendor lock-in;
- inadequate management of access rights;
- risks associated with the use of sub-processors;
- non-compliance with data retention restrictions;
- difficulties with accommodating data subjects' rights;
- unavailability of the services;
- difficulties with recovering data in the case of termination of the cloud provider's business or the service contract; and
- violations of data transfer restrictions.

To address these risks, the DPA has issued several guidelines for data controllers that want to migrate data to a cloud environment. The DPA recommends data controllers, among others, to:

- clearly identify data and data processing activities before migrating them to the cloud environment, considering the nature and sensitivity of the data;
- impose appropriate contractual and technical requirements on cloud providers (eg, not allowing cloud providers to alter terms and conditions unilaterally, requiring cloud providers to inform about the use of sub-processors and including exhaustive lists of physical locations where data can be stored);
- identify the most suitable cloud solution;
- perform a risk analysis (ideally by an independent body specialised in information security);
- select the appropriate cloud provider, considering the risk analysis;
- inform data subjects about the migration of their PI to the cloud; and
- monitor changes to cloud services over time and update the risk analysis in light of such changes.

On 20 May 2021, the DPA, as the lead authority, approved the EU Data Protection Code of Conduct for Cloud Service Providers (the EU Cloud CoC). The EU Cloud CoC creates a baseline for the implementation of the GDPR for the cloud market.

HUNTON ANDREWS KURTH

David Dumont
ddumont@huntonak.com

Laura Léonard
lleonard@huntonak.com

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
Tel: +32 2643 5800
Fax: +32 2643 5822
www.huntonak.com

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Data Protection Authority (DPA) published Recommendation 01/2021 on the processing of biometric data.

The DPA continued publishing materials, guidelines and adopting opinions on the processing of PI in the context of the coronavirus pandemic. Coronavirus-related content is available on the DPA's website.

Brazil

Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher, Thiago Luís Sombra and Luiz Felipe Di Sessa*

Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Brazilian Federal Constitution grants protection to the intimacy, private life, honour and image of the individual as a fundamental right (section 5, X of the Brazilian Federal Constitution). In the legal sphere, historically, Brazil has adopted a sectorial regulation on privacy, data protection and cybersecurity matters.

More recently, the Brazilian Congress passed a general data protection law (Law No. 13,709/2018 (LGPD), which has significantly transformed the data protection system in Brazil. The LGPD is inspired by the EU's data protection framework, particularly the General Data Protection Regulation (GDPR). On 8 July 2019, the president sanctioned Law No. 13,853/2019, which created the National Data Protection Authority (ANPD) and amended certain provisions of the LGPD.

The LGPD entered into force in September 2020. It establishes detailed rules for the collection, use, processing and storage of personal data and will affect all sectors of the economy, including the relationship between customers and suppliers of products and services, employees and employers, transnational and national commercial relations, as well as other relations in which personal data is collected in the digital environment or outside the digital environment.

In light of the covid-19 pandemic, the Brazilian Congress passed Law No. 14,010/2020 that, among other things, postponed the enforceability of the administrative sanctions provided for by the LGPD to August 2021. Since then, the administrative sanctions have officially been in force.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The ANPD is the government agency with technical autonomy but connected to the Cabinet of the Presidency, responsible for overseeing, issuing guidelines and enforcing the LGPD. Law No. 13,853/2019 expressly provides that ANPD has exclusive jurisdiction in relation to LGPD and, concerning the protection of personal data, such jurisdiction shall prevail over other public entities or organisations. Additionally, Decree No. 10,474/2020 regulates the governance structure of the ANPD and sets forth the responsibilities of the board of directors and other bodies that are part of the ANPD. In January 2021, the ANPD issued its regulatory agenda, which addresses actions considered to be the top priorities for LGPD regulation until the end of 2022.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The LGPD provides that the ANPD shall cooperate with other government bodies in relation to data protection matters but shall remain the central body concerning the interpretation of the LGPD. In addition, the ANPD has jurisdiction to promote cooperation actions with data protection authorities of other countries or international agencies.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection law may lead to administrative investigations handled by the ANPD, which shall grant the right to present a defence and an appeal, and may result in administrative sanctions. Breaches to data protection law do not normally lead to criminal penalties or liability. The sanctions that may be applied by the ANPD are the following:

- warnings, which will include a deadline for the adoption of corrective measures;
- a one-time fine of up to 2 per cent of the net turnover of the infringing entity's conglomerate in Brazil in its preceding fiscal year, excluding taxes, up to 50 million reais per violation;
- a daily fine, which is also subject to the limits set before;
- disclosures of the violation after it is verified, and its occurrence confirmed;
- the blocking of personal data corresponding to the violation until the controller's processing operations are brought into compliance;
- elimination of personal data corresponding to the violation;
- the partial suspension of the database to which the infraction refers for six months, extendable for another six months;
- the suspension of the data processing activity to which the infraction refers for six months, extendable for another six months; and
- a partial or complete prohibition of any data processing activities.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Under the Brazilian legal framework, all administrative decisions can be challenged in court, which include the ANPD's orders issued against data processing agents.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Law No. 13,709/2018 (LGPD) does not apply to the processing of personal data performed exclusively:

- by individuals for private and non-economic purposes;
- for journalistic, artistic or academic purposes;
- processing activities carried out exclusively for public security, national defence or state security;
- for public and state security or national defence purposes; and
- for investigation and prosecution of criminal offences.

Processing operations involving personal data originated in other countries or for other countries that only pass through the national territory without any other processing operation carried out in Brazil are also not subject to the LGPD. Except for the foregoing, the LGPD covers all sectors and types of organisations. It has not revoked other sector-specific legislation that shall continue to apply.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The LGPD mainly covers matters related to electronic marketing or monitoring and the surveillance of individuals. But other laws also address these issues.

The Civil Rights Framework for Internet in Brazil is Law No. 12,965/14 (the Internet Act), which outlines that the storage and availability of the connection and access logs to Internet applications, as well as of personal data and the contents of private communications, must observe intimacy, private life, honour and image of the parties directly or indirectly involved. The content of private communications may only be provided by a court order, as provided by law.

The confidentiality of telephone and computer communications is protected under the Wiretap Act (Law No. 9,296/96) and the Telecommunications Act (Law No. 9,472/97). The Wiretap Act provides that the access to and interception of telephone and telematics communications may only occur under the authority of a valid court order in criminal investigation proceedings. The Telecommunications Act provides that clients' information can only be used for the purpose of delivering services and that telecom bills can only be revealed upon the express consent of the user or by a valid court order.

On electronic marketing, Brazil has the Self-Regulation Code for Email Marketing Practice 2009 (the Email Code) that representative entities of marketing companies, internet service providers and consumers have signed. The Email Code permits electronic marketing with opt-in and soft opt-in (when there is any evidence of a previous commercial relationship between the sender and recipient). For these cases, senders do not need express consent from recipients but must provide an option to opt out. Although before the LGPD, the Email Code is consistent with the LGPD, as organisations may rely on consent (opt-in) or legitimate interest (soft opt-in) to justify the sending of electronic communications.

Concerning the monitoring and surveillance of individuals, labour precedents establish some rules on the monitoring of employees. Generally, court decisions uphold that the monitoring of computer systems made available to employees is allowed. Therefore, IT resources made available for the exercise of the employees' functions may be subject to surveillance. The surveillance of employees' personal devices may be possible (eg, in the event a professional email account is installed in the employee's mobile phone or computer) to the extent that it focuses only on the company's information. Employees' personal email shall not be monitored or accessed by the employer, and employees shall be informed in advance by their employer about all monitoring activities performed.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Data processing on the internet

The Internet Act establishes rules applicable to internet services and applications. Under the Internet Act, access logs to the internet and internet applications shall be retained for a period of 12 and six months, respectively.

Employee monitoring

Generally, court decisions sustain that the monitoring of computer systems made available to employees is allowed. Therefore, IT resources made available for the exercise of the employees' functions may be subject to surveillance. The surveillance of employees' personal devices may be possible (eg, in the event a professional email account is installed in the employee's mobile phone or computer) to the extent that it focuses only on the company's information. Employees' personal email shall not be monitored or accessed by the employer, and employees shall be informed in advance by their employer about all monitoring activities performed.

Health

The Medical Ethical Conduct Code (Federal Council of Medicine, Resolution No. 2,217/18) provides for certain rules on the protection of patients' information and medical records. Except for limited exceptions, the patient's data may only be disclosed to third parties with his or her written consent. Also, the Federal Council of Medicine governs the use of computer systems for storage, handling and retention of such data, authorising the electronic storage of documentation instead of paper. Electronic Medical Chart Law (Law No. 13,787/2018) provides for the digitalisation and use of computerised systems for storing and handling patient records. The Ministry of Health and the National Health Surveillance Agency (ANVISA) provide for specific rules applicable to data processing activities in clinical trials. Recently, Resolution No. 2.314/2022, issued by the Federal Council of Medicine, and Resolution No. 696/2022, issued by the Federal Council of Nusing, established new rules for telemedicine and tele-nursing, which include the protection of personal data in line with the obligations provided by the LGPD.

Banking

Pursuant to Bank Secrecy Act (Complementary Law No. 105/01), financial institutions, such as banks, credit card administrators and the stock exchange must maintain strict confidentiality of financial transactions and financial information of their clients. Resolution Nos. 4,480 and 4,474, of 2016, issued by the National Monetary Council have regulated, respectively, the opening and closing of bank accounts by electronic means and the digitalisation of documents, providing

for specific cybersecurity rules to ensure privacy in those situations. Resolution No. 4,893/2021, recently issued by the National Monetary Council, replaces Resolution No. 4,658/2018 and determines that financial institutions shall implement and maintain a cybersecurity policy, an incident plan and observe certain requirements for engaging data processing, storage and cloud service providers. Similar to Resolution No. 4,893/2021, Circular 3,909/2018 establishes the same cybersecurity rules for payment institutions. Finally, Joint Resolution No. 1/2020 issued by the National Monetary Council and the Central Bank sets forth the rules for the standardised sharing of data and services by means of opening and integrating platforms and infrastructures of information systems (ie, open banking).

Concession of credit

The Good Payer's Database Act (Law No. 12.414/11) regulates the creation and consultation by third parties of a central database containing credit scoring and payment history information of natural or legal persons for the purposes of building a credit history. Any legal entity or individual may consult such database to support its credit risk analysis, and decisions on the granting of credit, payment in instalments or other commercial and business transactions that involve financial risk to the consultant of such database. Decree No. 9.936/2019 regulates the Good Payor's Database Act, establishing complementary rules for the creation of a central database for the purposes of building credit history, including the obligations and responsibilities of the parties involved, data subject's rights, transparency requirements and notification requirements in the case of a data breach.

Government

The Information Access Act (Law No. 12,527/11) governs the use and processing of data by the public administration and establishes rules and procedures by which individuals may request details of the information collected by the public administration.

PI formats

9 | What categories and types of PI are covered by the law?

The LGPD defines 'personal data' as information related to an identified or identifiable natural person, and any processing of such personal data carried out by any form, whether in the digital media or physical environment.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

No. The LGPD has significant extraterritorial reach, applying to any processing activity carried out within the Brazilian territory and out of the Brazilian territory, regardless of where the processing agents are domiciled or the data are located, as long as:

- the purpose of the processing activity is to offer or provide goods or services in Brazilian territory;
- the purpose of the processing activity is to process personal data of individuals located in Brazilian territory; and
- the personal data is collected in Brazilian territory.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The definition of 'processing' established in the LGPD encompasses almost any activity performed with personal data. In both statutes 'processing' is defined as any operation performed with personal data, such as those that concern the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or information control, modification, communication, transfer, dissemination or extraction. In practical terms, any processing operation with personal data shall be subject to the LGPD.

Also under the LGPD, processing agents may be defined as controllers or processors. The controller is the natural or legal person, whether public or private, who is responsible for decisions concerning the processing of personal data. The processor is a natural or legal person, whether public or private, who performs the processing of personal data on behalf of the controller and only under the controller's instructions.

The controller has more obligations than the processor, but both must follow some duties equally. There is neither a definition nor a distinction of requirements to those that own PI.

For example, controllers and processors must:

- abide by data processing principles provided in the LGPD; and
- adopt technical and organisational measures to protect personal data from data incidents.

For example, controllers must:

- appoint a data protection officer (DPO);
- make easily accessible information to the data subject on how personal data is processed;
- justify and document the data processing in one of the 10 lawful bases outlined in the LGPD, which include, but are not limited to:
  - the consent of the data subject;
  - compliance with a legal obligation;
  - performance of a contract;
  - legitimate interest; and
  - sensitive data;
- justify and document the lawful bases for transfer of data out of the country, when applicable;
- comply with the data subject's rights;
- perform privacy impact assessments, when required;
- comply with the specific requirements for obtaining the consent and processing children's personal data; and
- notify the data protection authority in the event of an incident, such as unauthorised disclosure or use of personal data.

Both controllers and processors may be jointly and severally liable for the processing data in activities in which they are involved.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

According to Law No. 13,709/2018 (LGPD), personal data can only be processed and collected when justified in one of the 10 legal bases, which are:

- consent of the data subject: the LGPD requires the consent to be a prior, free, informed and unambiguous manifestation of the data subject, for a specific purpose. It shall be provided in writing or by another demonstrable means, showing the data subject's intention. If the data subject's consent is given by a written declaration, the request for consent shall be presented in a manner clearly distinguishable from the others. Generic authorisations for data processing are considered null and void;
- when necessary for the performance of a contract or preliminary understandings;
- when necessary to comply with legal or regulatory obligations imposed on the controller;
- based on the legitimate interest of the controller or third parties, if the interest or the fundamental rights and freedoms of the data subject are not overridden by such legitimate interest;
- when necessary for the protection of credit;
- exercise of rights during a court, administrative or arbitration proceeding;
- when necessary for the protection of life or physical integrity of the data subject or third party;
- when necessary for the protection of health, exclusively in procedures conducted by healthcare professionals, health services and sanitary authorities;
- for research and studies conducted by non-profit research entities; and
- by the government to perform public policies.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

The LGPD establishes a more stringent lawful basis for processing sensitive data. Sensitive personal data is personal data related to an individual in connection with racial or ethnic origin, religious belief, political opinion, trade union, philosophical or political organisation affiliation, health data, sexual life, genetic or biometric data. Processing sensitive personal data may only be carried out:

- with specific consent, which must be provided separately from other consents that might be sought; or
- without consent, in case the processing is required for:
  - compliance with a legal or regulatory obligation;
  - protecting life or the physical safety of the data subject or third parties;
  - lawful exercise of rights, including in contracts and connection with judicial, arbitral or administrative proceedings;
  - protection of health, exclusively in procedures conducted by healthcare professionals, health services and sanitary authorities; or
  - ensuring fraud prevention and data subject's authenticity, in electronic systems.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Data controllers must provide data subjects with specific information regarding the processing of their personal data. This information can be made available to the data subject through an easily accessible and detailed privacy notice. The privacy notice must contain clear, adequate and ostensive information including, but not limited to:

- specific purposes of the data processing; form and duration of the data processing;
- identification and contact information of the controller;
- information regarding the shared use of personal data by the controller, to whom and the purpose of why data is shared;
- responsibilities of the processing agents; and
- rights of the data subjects.

The privacy notice should be made available to data subjects preferably before the data processing activities take place. If this is not possible, the document should be made available at the very first opportunity.

If requested by the data subject, controllers shall inform and provide to the data subject the personal data they hold. Security incidents that may entail significant risk or damage to data subjects may have to be communicated to the data subject.

Exemptions from transparency obligations

15 | When is notice not required?

There is no express exception to the requirement of making available clear and complete information to data subjects. As a rule, such requirement must always be fulfilled. However, under very limited circumstances where making the information available beforehand is impossible (eg, when the personal data is collected from public sources), controllers may consider the possibility of processing the personal data and only providing the mandatory information to data subjects if required by them. In these cases, controllers should conduct an assessment on a case-by-case basis to identify potential risks of breach of the data protection rules.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes, the LGPD lists a series of principles that must govern every data processing activity, including:

- data quality: controllers must guarantee that data subjects' data is accurate, clear, exact and pertinent considering the necessity and purposes of the data processing activity. Data subjects have the right to update their personal data. In this regard, to the extent possible, data subjects should also be proactive with respect to updating their data before processing agents; and
- adequacy: data processing activities must be compatible with the purposes informed to the data subject.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The law does not restrict the types or volume of PI that may be collected in a specific manner. However, under the LGPD, data processing agents must respect the necessity principle, which imposes limits to the processing of personal data. According to such principle, the processing of personal data must be limited to the minimum necessary for fulling the purpose of the processing activity. In this regard, the data processed must be appropriate, proportional and not excessive to achieve the purposes of interest.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The LGPD does not restrict the amount of PI that may be held by controllers and processors. However, under the necessity principle, personal data should only be processed to the extent that it is necessary to achieve the purposes informed to the data subjects. Similarly, under the data minimisation principle, controllers should only keep the minimum amount of PI that is needed to accomplish such purposes. As a result, any personal data that is not necessary or that is excessive to achieve a certain purpose should not be collected or should be excluded or anonymised, as the case may be.

The LGPD does not restrict the length of time for which PI may be held either. Nevertheless, it establishes that the processing of personal data shall end when:

- it has achieved its purposes, or the data is not necessary or relevant for the purpose it was collected;
- the processing is finished;
- the data subject withdraws his or her consent and there is no other legal basis that is capable of justifying the continuity of the data processing activity; and
- the national authority determines so.

While determining the length of time for which PI should be held, controllers and processors should bear in mind any regulatory or legal obligation related to the maintenance of data, as well as any applicable statute of limitations that could impact their retention policies.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes. According to the purpose limitation principle imposed by the LGPD, the processing of personal data must be carried out for legitimate, specific and explicit purposes, and the data subject must be informed. Data processing agents cannot process the personal data for a purpose that was not informed to the data subjects.

If the purpose has changed, the controller must inform the individual and observe whether the legal basis initially adopted is still compatible with the new purpose. Besides, publicly available personal data may be processed for new purposes, subject to the legitimate purposes of the new processing activity and the rights of the data subject, as well as the principles established by the LGPD.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

There is no specific restriction related to the use of PI to make automated decisions without human intervention. However, the LGPD establishes that the data subject shall have the right to request the review of automated decision-making based on personal data when the decision can affect its interests, including decisions to define aspects of data subjects' personal, professional, consumer or credit profile or aspects of his or her personality. The LGPD does not regulate if the review of the decision must be carried out by a human or can be done by a new automated process.

In addition, the data controller must provide clear and adequate information about the criteria and procedures adopted for making these decisions.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Controllers and processors must adopt technical and organisational security measures, to protect PI from unauthorised access and accidental or illegal destruction, loss, change, communication or dissemination events, or any other event resulting from inappropriate or unlawful processing.

The National Data Protection Authority (ANPD) may provide minimum technical standards, taking into account the nature of the data, the specific characteristics of the processing and the current state of technology, especially in the case of sensitive personal data.

Also, Law No. 13,709/2018 (LGPD) establishes that such measures shall be applied from the conception phase of the product or service through its execution (privacy-by-design). The systems used for processing personal data shall be structured to meet the security requirements, standards of good practice and governance, general principles provided in the LGPD and other regulatory rules.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Yes. Data incidents that may entail significant risk or damage to data subjects must be communicated to the ANPD, the data subject and specific regulatory bodies (depending on the nature of the data subject to the data breach and on the regulatory requirements applicable). Although there is no formal regulation about timing requirements, the ANPD recommends that the notification should be provided within two days of it becoming aware of the breach.

The notification must contain, at least, the following:

- a description of the nature of the personal data affected;
- the categories of affected data subjects;
- the technical and security measures adopted;
- the risks related to the incident;
- the reasons for any delayed communication, if applicable; and
- the measures adopted to revert or mitigate the effects of the damage caused by the incident.

Additionally, Decree No. 9,936/2019, which regulates the Good Payer's Database Act, outlines that credit reporting agencies (ie, as a legal entity responsible for the administration (collection, storage, analysis and concession of access to) of data related to a natural or legal person for the purposes of supporting the concession of credit, payment in instalments or other commercial and business transactions that entails financial risk) must report a data breach that might create risk or relevant damage to the data subjects within two business days of it becoming aware of the breach. Breaches involving good payer's data must be reported to:

- the National Data Protection Authority, if the breach involves personal data;
- the Central Bank, if the breach involves data provided by regulated institutions; and
- the Secretariat for Consumer Protection, if the breach involves consumer data.

The notification must contain, at least, the following:

- a description of the nature of the personal data affected;

- the categories of affected data subjects;
- the technical and security measures adopted;
- the risks related to the incident; and
- the measures adopted to revert or mitigate the effects of the damage caused by the incident.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Yes. Law No. 13,709/2018 (LGPD) establishes that data processing agents (controllers and processors) must maintain records of their data processing operations, especially when based on legitimate interest. In addition, the LGPD sets forth that the controller and the processor must adopt technical and administrative security measures capable of protecting personal data from unauthorised access and accidental or illegal destruction, loss, change, communication or dissemination events, or any other occurrence resulting from inappropriate or illegal processing.

These obligations are in line with the accountability principle provided by the LGPD, which determines that it is the responsibility of the controller and the processor to demonstrate the compliance of their data processing activities with the LGPD.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

As a rule, it is mandatory to appoint a data protection officer (DPO). However, the National Data Protection Authority (ANPD) enacted Resolution CD/ANPD No. 2/2022, which exempts small businesses – as defined by the Resolution – from appointing a DPO. This is the only exemption to the appointment of a DPO to date.

Both controllers and processors should designate a DPO. The DPO is the communication channel between the controller or processor, the data subject and the ANPD. According to the LGPD, the DPO's legal responsibilities are:

- accepting complaints and notifications from the data subjects, providing them with clarifications and adopting the related necessary measures;
- receiving notifications or communications from the ANPD and adopting the necessary measures;
- providing advice to the entity's employees and contractors regarding practices to be observed in relation to the protection of personal data; and
- performing any other activities determined by the controller or established in complementary standards issued by the ANPD.

On the criteria for appointing a DPO, the LGPD is silent on whether the DPO should be an individual or a legal entity; an employee of the organisation or an external agent; or a qualified professional in the data protection field or not.

In any event, the ANPD has published its Guidelines on Data Processing Agents, which are not binding and are subject to review, whereby it adopted the following:

- the DPO can be either an employee or an external agent;
- the DPO can be an individual or a legal entity;
- to assess the DPO's qualification, controllers and processors should consider if the DPO's data protection and information security knowledge meets the needs of the organisation's personal data processing activities;
- the DPO can be supported by a team;
- an individual or legal entity can be designated as DPO of more than one controller or processor, provided that there are no conflicts of interest involved and that the DPO is satisfactorily available to carry out all its activities; and
- the DPO should be an individual or legal entity with a reasonable level of autonomy to carry out its activities.

The ANPD is expected to enact complementary rules regarding the definition, role and responsibilities of the DPO.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Controllers and processors must keep accurate and updated records of processing activities (ROPAs) carried out by them. The ANPD may request controllers and processors to present their ROPAs at its own discretion and may audit data processing agents to verify if the ROPAs are accurate. The ANPD is expected to further regulate the legal requirements applicable to ROPAs.

Risk assessment

26 Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The LGPD determines that the controller must carry out a data protection impact assessment (DPIA) when requested by the ANPD. However, the LGPD does not expressly define in which moment the DPIA must be produced. In turn, it highlights two hypotheses under which the ANPD may request this documentation: when the processing is based on legitimate interest; and in broad terms, the ANPD may request the controller to produce the DPIA, including when processing involves sensitive data, pursuant to specific regulation.

For these reasons, we understand that, at present, there is no mandatory obligation for the controller to produce the DPIA proactively for each relevant data processing activity and when relying on legitimate interest. The duty imposed on the controller is to deliver such documentation for the ANPD when requested. However, in compliance with good corporate governance practices, we understand that the proactive elaboration of the DPIA is recommended as it may demonstrate that the controller has strong data governance and it may help to mitigate the chances of exposing the rights and freedoms of data subjects and, consequently, of violating the LGPD.

The DPIA must contain, at least, a description of the personal data processing operations that may result in risks to civil liberties and fundamental rights, as well as measures, safeguards and risk-mitigation mechanisms.

In addition, the LGPD sets forth the legal basis of the legitimate interest of the controller or a third party for the processing of personal data, except in cases where the data subject's fundamental rights and freedoms that require the protection of personal data prevail. In this regard, the ANPD has already stated in a public technical note that the analysis of when the legitimate interest may justify processing operations must imply a balancing test to analyse if the privacy rights of the data subjects shall prevail. Additionally, the ANPD has stated, in the Guidelines for the application of the LGPD by processing agents in the electoral context, that the controller must conduct a prior assessment to

the data processing activity. According to this document, the controller must verify:

- the legitimacy of the interest of the controller or the third parties;
- the proportionality between such interest and the rights and legitimate expectations of data subjects; and
- the adoption of technical and administrative measures capable of safeguarding the operation, the data processed and the rights of data subjects.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Both controllers and processors must adopt security measures suitable to protect personal data, and such measures must be applied from the conception phase of the product or service through to its execution, requiring organisations to adopt a privacy-by-design approach.

In circumstances to be determined by the ANPD, the controller must produce a privacy impact assessment.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

No. Under Law No. 13,709/2018 (LGPD) it is not necessary to register the controller, the processor, the database, or any other document or processing activity with the National Data Protection Authority.

Other transparency duties

29 | Are there any other public transparency duties?

There are no specific transparency requirements before the processing activity, such as making public statements regarding the nature of the processing. However, 'transparency' is one of the underlying principles of the LGPD that governs every data processing activity. According to this principle, clear, precise and easily accessible information shall be made available to data subjects whose data is being processed.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Law No. 13,709/2018 (LGPD) does not provide for any specific requirements for outsourcing data processing services. It outlines general obligations for both controllers and processors.

The LGPD establishes a joint and severe liability regime to controllers and processors for any unlawful processing.

Sector-specific regulation may establish requirements for outsourcing processing services.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Besides general requirements of transparency, notice and purpose limitation, the LGPD specifically prohibits the disclosure or shared use of health data – deemed sensitive data – to obtain financial gain, except in specific circumstances, such as for the provision of health services, pharmaceutical care or healthcare. The sharing of other types of sensitive data to obtain financial gain may be restricted by the National Data Protection Authority (ANPD) in future regulation. Sector-specific laws may impose additional requirements or prohibitions on the disclosure of personal data.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The LGPD expressly determines the cases in which an international transfer of data is permitted, which are detailed below:

- to countries or international organisations that offer an adequate level of personal data protection as established in the LGPD;
- when the controller offers and demonstrates compliance with principles in the LGPD, the data subject's rights and the data protection system established in the law, through specific contractual clauses for a given transfer, standard contractual clauses, binding corporate rules or regularly issued seals, certificates and codes of conduct (all of which shall be previously regulated or approved by the ANPD);
- when the transfer is necessary for international legal cooperation between government intelligence, investigations, and prosecution authorities, according to instruments of international law, or when it is the result of a commitment established in an international cooperation agreement;
- when the transfer is authorised by the ANPD;
- when the transfer is necessary for the execution of public policies or public service activities;
- when the data subject has provided specific and highlighted consent for the transfer upon prior information regarding the international character of the activity, clearly distinguishing this from other purposes for data processing;
- when necessary for the protection of life or physical integrity of the data subject or third party;
- when it is necessary for the fulfilment of a legal or regulatory obligation on the part of the controller;
- for the execution of a contract or procedures related to the contract in which the data subject is a party, as long as required by the data subject him or herself; and
- for the regular exercise of rights in court and administrative or arbitration proceedings.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes. The restrictions on international data transfer apply equally to any data-sharing operation with a recipient located abroad, regardless of whether the recipient is a data processor or a data controller or whether the transfer will occur once or continuously.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no general data localisation requirements in Brazil. The only regulation that requires the maintenance of certain PI or a copy of PI in Brazil is Ordinance No. 05/2021 of the Cabinet of Institutional Security, which imposes minimum data security requirements for adopting cloud computing solutions by the federal government.

This Ordinance determines which information may be processed within a cloud environment (eg, classified information cannot be processed in this environment in any case) and establishes that, as a rule, data, metadata, information or knowledge originated by an entity of the federal government must be hosted in Brazil. However, in specific circumstances (eg, processing of information without restriction of access), the data may be processed abroad provided that a backup is available in Brazil.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, Law No. 13,709/2018 (the LGPD) establishes that the data subject has the right to obtain confirmation of the existence of processing of his or her data and access to the personal data at any time. This can occur in two different ways:

- in simplified form, if the confirmation or access is provided immediately; or
- by means of a clear and complete statement, indicating the origin of the data, non-existence of records, criteria used and purpose of the processing, as the case may be, within 15 days counted from the date of the request.

The information will be provided free of charge, electronically or in hard copy, in accordance with the data subject's request.

Also, when the processing of data is a result of a consent or a contract, the data subject may ask for a complete electronic copy of his or her personal data.

Other rights

36 | Do individuals have other substantive rights?

Besides the right to confirm the existence of or have access to data collected, the LGPD outlines the following data subject rights:

- the right to correct incomplete, inaccurate or outdated data;
- the right to have their personal data blocked, deleted or anonymised when the data processing is excessive or unlawful;
- the right to portability;
- the right to withdraw previously granted consent for processing their personal data;
- the right to have their personal data deleted when consent has been withdrawn;
- the right to information about the public or private entities with whom the controller has shared the personal data;
- the right to information about the possibility to not provide consent and the eventual negative consequences;
- the right to oppose to the unlawful processing of their personal data if the processing was based on one of the cases in which consent is waived; and
- when the data processing is exclusively based on automated decisions that might affect the data subjects' rights, the data subject has the right to request the review of such a decision.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes, any harm caused to individuals, both of material and moral nature, may trigger liability. Evidence of actual damage is not necessarily required to grant indemnification to data subjects.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Both. All the rights and obligations outlined in the LGPD and other privacy related laws are enforceable in the administrative sphere, by the National Data Protection Authority and in court, individually or collectively.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

No.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

There is no rule specifically dealing with the use of cookies or other equivalent technologies. The use of personal data through cookies and other tracking technologies (such as fingerprinting) are generally subject to the rules imposed by Law No. 13,709/2018 (LGPD) and Law No. 12,965/14 (the Internet Act).

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

There is no binding and specific email marketing or anti-spam legislation in place. This type of activity usually falls under general privacy regulation.

The telecommunications regulators determined that mobile carriers are only allowed to send promotional messages to users who have expressly accepted receiving them. The Brazilian Court of Justice has ruled that telephone marketing without the prior consent of the consumer is considered an abusive practice.

Other regulations have been discussed with the goal of protecting individuals from undue or excessive marketing communications. For instance, Decree No. 11.034/2022, which regulates customer service, prohibits telephone marketing while the consumer is waiting for the service, unless the consumer has previously consented. In addition, the state of São Paulo approved Law No. 17,334/2021, a law that creates a registration channel so consumers can block the receipt of telemarketing communications.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules on targeted online advertising in place. This type of activity usually falls under general privacy regulations (such as by consumer protection legislation).

From a data protection perspective, data processing agents must observe data protection principles, such as those of non-discrimination, transparency and information self-determination. In addition, as targeted online advertising usually involves the processing of personal data in a more extensive way, controllers should carry out a careful assessment to choose the applicable legal basis to justify such data processing activities and ensure that data subject rights are respected.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The LGPD establishes a more stringent lawful basis for processing sensitive data. For instance, the legal basis of legitimate interest and credit protection cannot be used to justify the processing of sensitive data. Further, the sharing of sensitive data may be restricted or prohibited in certain cases.

Profiling

44 | Are there any rules regarding individual profiling?

The LGPD and other Brazilian laws do not specifically regulate profiling activities. However, to comply with LGPD principles, the data controller that intends to carry out profiling activities must, at least,

- ensure the provision of clear information to the data subject about this processing;
- avoid processing data that may be deemed non-proportional or excessive in relation to the intended purpose; and
- ensure that the profiling activity will not result in illegal or abusive discriminatory practice.

Despite the fact that profiling is not specifically regulated, the LGPD regulates automated decision-making, which is an essential part of the profiling. The data subject has the right to request a review of an automated decision made solely on the basis of automated processing (ie, without human intervention) when it affects their interests.

Moreover, it establishes that the controller must provide, whenever requested, clear and adequate information regarding the criteria and the data procedures used for the automated decision, respecting commercial and industrial secrecy.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Currently, in Brazil, there is no specific law to regulate cloud services. However, several rules may affect the use of cloud services, such as:

- Financial and Payment Institutions: CMN Resolution No. 4.893/2021 and BCB Resolution No. 85/2021 establish requirements for hiring data processing, data storage and cloud computing services to be observed by financial and payment institutions.
- Government: Ordinance No. 05/2021 provides guidelines, principles and duties on information security applicable to the processing of information in the cloud environment by the Federal Public Administration (FPA). According to the Ordinance, certain data, metadata, information and knowledge, produced or stored by FPA bodies, as well as its backups must reside in the Brazilian territory. In addition, the guidelines of Decree No. 9.637/2018 must be considered when the public administration plans to procure cloud services.

MATTOS FILHO >
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Fabio Ferreira Kujawski
kujawski@mattosfilho.com.br

Paulo Marcos Rodrigues Brancher
pbrancher@mattosfilho.com.br

Thiago Luís Sombra
thiago.sombra@mattosfilho.com.br

Luiz Felipe Di Sessa
luiz.sessa@mattosfilho.com.br

Alameda Joaquim Eugênio de Lima
447 Jardim Paulista
São Paulo, SP 01403 001
Brazil
Tel: +55 11 3147 7600
www.mattosfilho.com.br

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Law No. 13,709/2018 (LGPD) is the first general data protection law; therefore, there is a lot of debate regarding how to become compliant with it and how it will be enforced by the National Data Protection Authority (ANPD). In this regard, becoming compliant with the LGPD has shown to be a significant challenge to both Brazilian and foreign organisations, including those with or without established privacy teams.

The ANPD published a regulatory schedule, which lists the first topics that the ANPD intends to regulate. It includes, for instance, the beginning of the regulation on international data transfer in Q1 of 2022. In addition, under this regulatory schedule, the ANPD already published a regulation regarding the applicability of sanctions and the special regime granted to small and medium-sized enterprises.

As the ANPD is issuing and studying new regulations, the increase in regulatory scrutiny on data protection and privacy issues is expected. Given the nature of the obligations set forth by the LGPD, organisations should be especially aware of those relating to data subjects' rights and data breaches.

* *The authors would like to thank Jaqueline Simas de Oliveira, Isabela Fernandes Pereira and Nuria Baxauli for their contributions to the chapter.*

Canada

B Douglas Tait and Kendall N Dyck

Thompson Dorfman Sweatman LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

In Canada, four private sector privacy enactments provide the framework for the protection of PI. These are:

- Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA);
- the province of Quebec's An Act Respecting the Protection of Personal Information in the Private Sector (Private Sector Act (QC));
- the province of Alberta's Personal Information Protection Act (PIPA (AB)); and
- the province of British Columbia's Personal Information Protection Act (PIPA (BC)).

PIPEDA governs the interprovincial and international collection, use or disclosure of PI by private sector organisations in the course of carrying out commercial activities for profit. It also has application to employee PI in federally regulated organisations (such as banks, airlines, railways and telecommunication companies).

PIPEDA also applies within all provinces and territories in Canada, except Quebec, Alberta and British Columbia. The Private Sector Act (QC), PIPA (AB) and PIPA (BC) have been deemed substantially similar to PIPEDA and, as such, PIPEDA does not apply to private sector organisations carrying out commercial activities wholly within those provinces.

While the Private Sector Act (QC), PIPA (AB) and PIPA (BC) have each been deemed substantially similar to PIPEDA, there are differences in the details of each. These provincial laws apply, generally speaking, to all private sector organisations with respect to the collection, use and disclosure of PI in the course of carrying out commercial activities and to employees' PI.

The Private Sector Act (QC) has recently been amended by Bill 64, which introduced significant changes that will come into effect in 2022, 2023 and 2024. While it does not address territorial scope, it is drafted broadly and includes new obligations that suggest it may be applied to organisations outside of Quebec that deal with the PI of Quebec residents. For example, a new requirement to conduct a privacy impact assessment when PI of Quebec residents is being transferred outside of Quebec, or where an organisation has entrusted a third party located outside Quebec with the collecting, using, disclosing or retaining PI on its behalf.

Health information privacy legislation in the provinces of Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador have been deemed substantially similar to PIPEDA and apply to health PI within those provinces. In those provinces and territories where health information privacy legislation has not been deemed substantially similar, PIPEDA may also apply.

Privacy matters involving public sector institutions are governed by a variety of federal, provincial and territorial public sector privacy legislative enactments.

Certain provinces have enacted legislation recognising the invasion of privacy as statutory tort, while there are also various offences within the Criminal Code (Canada) regarding the invasion of privacy.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

There is no single regulatory authority dedicated to governing data protection laws in Canada. The applicable authority varies based upon whether the matter is covered by federal or provincial privacy laws.

While the Office of the Privacy Commissioner of Canada (OPC) enforces PIPEDA, each province and territory of Canada has a commissioner or ombudsperson responsible for its own provincial or territorial privacy legislation. In the case of Quebec, Alberta and British Columbia, their privacy legislation is overseen and enforced by the Commission d'accès à l'information du Québec (CAI), the Office of the Information & Privacy Commissioner of Alberta and the Office of the Information & Privacy Commissioner for British Columbia, respectively.

Under PIPEDA, the OPC has the power to investigate complaints made by individuals or initiate an investigation itself based on reasonable grounds to believe that a matter warrants it. The OPC has the power to summon witnesses to give oral or written evidence, inspect documents and compel the production thereof, and inspect premises other than a dwelling house. The OPC, upon having reasonable grounds to believe that an organisation is contravening PIPEDA, can audit the organisation's personal information practices, including examining their policies, procedures and practices, exploring their physical and security controls, and inspecting an organisation's incident response management protocols.

The CAI, under the Private Sector Act (QC), and the commissioners under PIPA (AB) and PIPA (BC) each have similar investigatory powers and, where necessary, the power to conduct an inquiry. Following an inquiry, each also has the power to issue orders.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There are no legal obligations on Canadian data protection authorities to cooperate with other data protection authorities. However, the OPC and the commissioners in the three provinces that have substantially similar

legislation (Quebec, BC and Alberta) have entered into a memorandum of understanding intended to create a framework for greater collaboration between the offices, streamline investigations and promote greater harmonisation in the application of the laws. The OPC may also share information with a foreign data protection counterpart pursuant to a written information sharing arrangement.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

In Canada, breaches of federal and provincial privacy laws can result in sanctions or orders, or criminal penalties.

Under PIPEDA, certain breaches can, if an organisation is found guilty, result in monetary fines. However, as it currently stands, the OPC does not have the authority under PIPEDA to prosecute offences or issue fines. As such, where it believes an offence has been committed, the matter must be referred to the office of the Attorney General of Canada, who, after its investigation, determines potential prosecution.

Effective 22 September 2023 the Private Sector Act (QC) will provide three different types of enforcement mechanisms: penal offences, administrative monetary penalties (AMPs) and a private right of action. The CAI will have the power to institute penal proceedings that may result in a fine of up to C$25 million or 4 per cent of worldwide turnover, which will be imposed by the Court of Quebec. A person designated by the CAI, but who is not a member of the CAI, will have the power to impose AMPs in certain circumstances of up to C$10 million or 2 per cent of worldwide turnover. Individuals will have the ability to claim punitive damages when organisations infringe their rights, causing an injury, either intentionally or from gross negligence.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Under PIPEDA, organisations have no right to appeal or seek judicial review of the findings or recommendations included in the OPC's report. This is likely because on their own, those findings and recommendations are not binding on the organisation. However, organisations and complainants have successfully challenged the OPC's conduct during an investigation through judicial review applications to the Federal Court under the Federal Courts Act in circumstances where an application to that Court could not otherwise be made under PIPEDA.

In Alberta and British Columbia, organisations have the right, exercisable within a prescribed time, to apply for judicial review or orders made under PIPA (AB) or PIPA (BC). In Quebec, an individual may appeal orders made under the Private Sector Act (QC) to a judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) applies only to PI collected, used or disclosed during a commercial transaction (with some exceptions), or relating to the employee of a federally regulated industry. It does not cover any private sector, for profit, commercial organisation operating wholly within the provinces of Quebec, Alberta and British Columbia, nor does it cover the PI of employees of private sector, for profit, commercial organisations that are not federally regulated. It also generally does not cover organisations that are not engaged in for profit commercial activities (such as not-for-profits, charities and political parties). Organisations that collect PI solely for 'journalistic, artistic or literary purposes' are also exempt from PIPEDA.

BC's Office of the Information and Privacy Commissioner (OIPC) recently received a complaint and conducted an investigation into whether its Personal Information Protection Act applied to the Conservative Party of Canada, the Green Party of Canada, the Liberal Party of Canada or the New Democratic Party of Canada. The OIPC found each is an organisation within the meaning of British Columbia's Personal Information Protection Act (PIPA), and PIPA (BC) is not inapplicable. That decision is currently the subject of judicial review.

Effective 22 September 2023, Quebec's An Act Respecting the Protection of Personal Information in the Private Sector (the Private Sector Act (QC)) will provide that political parties, independent members and independent candidates governed by Quebec's Election Act will be subject to the majority of the Private Sector Act (QC), with specific exceptions.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Electronic marketing is regulated by legislation commonly known as Canada's Anti-Spam Legislation (CASL). PIPEDA will apply to the same activities where the processing of personal information is involved.

Private sector privacy laws generally permit overt or covert video surveillance and the recording of phone calls, but both must be balanced with an individual's right to privacy and to achieve a specific purpose. As a general rule, organisations should consider less intrusive means of achieving the same end before conducting video surveillance. In addition, certain provinces have enacted statutory privacy torts for violation of privacy in which surveillance or the listening to, or recording of, a conversation may be a violation of an individual's privacy.

The Criminal Code sets out privacy-related offences, specifically the interception of communications and provisions governing how law enforcement may obtain judicial authorisation to conduct electronic surveillance for criminal investigations.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Numerous federal and provincial laws provide for specific privacy and data protection rules and laws that apply to, among other things, banking, credit unions, financial transactions, electronic commerce, consumer credit reporting, health and health records or data that contains specific confidentiality provisions concerning PI that is collected.

PI formats

9 | What categories and types of PI are covered by the law?

The basic concept in Canadian privacy law is that PI is any information, recorded or not, about an identifiable individual, regardless of what format it may be held in. Examples of PI are:

- age, name, assigned identification numbers, income, ethnic origin, religion, marital status, fingerprints or blood type;
- opinions, evaluations, comments, social status or disciplinary actions;
- education, medical, criminal and employment histories;

- information about financial transactions; and
- employee files, credit records, loan records and medical records.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

PIPEDA is silent as to its territorial scope. However, the Federal Court of Canada has held that, in the absence of language clearly limiting its application to Canada, PIPEDA can be interpreted to apply in all circumstances in which there exists a 'real and substantial link' between an organisation's activities and Canada.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Under PIPEDA, the organisation that determines the purpose of collection and collects, uses and discloses the PI is in control of that information. The same organisation may also process the PI itself or transfer it to a third party (either within or outside of Canada) for processing. Even though PI may be transferred to a third party for processing, it is the controlling organisation that remains in control of, and is ultimately responsible for, the PI.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

In general, subject to limited exceptions, Canadian private sector privacy legislation requires organisations to obtain meaningful consent for the collection, use and disclosure of PI. What constitutes 'meaningful consent' is guided by seven principles designed to ensure that the individual providing the consent has, among other things, a clear understanding of the nature, purpose and consequence of what they are consenting to, been provided information (in a clear and comprehensible manner) about the organisation's privacy management practices and been provided with a clear 'yes' or 'no' option.

Further, under the Personal Information Protection and Electronic Documents Act (PIPEDA), the purpose for which PI is collected, used or disclosed must be one that a reasonable person would consider appropriate in the circumstances. Otherwise, even with consent, the organisation will have violated PIPEDA.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Privacy legislation generally states that the more sensitive the PI, the greater the security safeguards required to protect it. It is up to an organisation to determine what is appropriate in the particular circumstances. The Office of the Privacy Commissioner of Canada, which oversees PIPEDA, has released guidance that states that while some information (health and financial, etc) is always considered sensitive and subject to more stringent protections, any PI could be considered sensitive depending on the context.

In addition, the vast majority of provinces have health legislation that applies specifically to entities that fit within the definition of 'custodians' or 'trustees' and have stricter and more specific standards of security safeguards for health PI.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Under Canadian private sector privacy law, meaningful consent (either express or implied) is necessary for an organisation's collection, use and disclosure of PI except in limited circumstances. For consent to be meaningful, individuals must understand the nature, purpose and consequences of what they are consenting to. Under Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA), organisations must inform individuals of their privacy management practices, with a particular emphasis on what PI is being collected, with which other organisations their PI might be shared, the purpose for the collection, use or disclosure, and the risk of harm and other consequences that might result from that collection, use or disclosure. Where an organisation is transferring PI to foreign jurisdictions for processing, it must notify the individual that such PI is subject to the laws of that country and may be lawfully accessed there.

In addition, organisations have a general obligation to be open about their policies and practices relating to the management of PI under PIPEDA. Organisations must make certain information readily available to the public in a way that is generally understandable. This includes the contact information of the individual accountable for the organisation's privacy practices, a description of the type of PI the organisation holds, how an individual can gain access to their PI, a general account of how the organisation uses the PI, what PI is shared with related organisations and a copy of information explaining the organisation's practices. This information typically shows up in website privacy policies, which can only be relied on for consent in certain circumstances (ie, where implied consent is appropriate) because they are often not available until after the collection or use has occurred.

Under PIPEDA, individuals are entitled to be informed of the existence, use and disclosure of their personal information by an organisation, and to access that information, upon making a request in writing. Where an organisation suffers a breach of their security safeguards that creates a real risk of significant harm to the impacted individuals, they must provide notice to the Office of the Privacy Commissioner of Canada (OPC) and those impacted individuals. The notification must be conspicuous and include enough information to allow the individual to understand the significance of the breach to them and to take steps, if possible, to reduce or mitigate the risk of harm.

Exemptions from transparency obligations

15 | When is notice not required?

Generally, Canadian private sector privacy law is based on consent, which necessarily requires that individuals be provided particular information on which to base their decision to provide or withhold consent to the collection, use or disclosure of their PI. PIPEDA outlines specific exceptions wherein collection, use or disclosure is allowed without the knowledge or consent of the individual. For example, where PI was produced by the individual in the course of their employment and the collection, use or disclosure is consistent with the purposes for which the information was produced. PI can also be collected without knowledge and consent where it would compromise the availability or accuracy of

the information and the collection is reasonable for purposes related to investigation a breach of contract or law. These are only a few examples.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Canadian privacy legislation contains obligations for organisations to ensure that the PI that it uses, collects and discloses is accurate, complete and up to date, particularly where the information is used to make a decision about the individual to whom the information relates or is likely to be disclosed to another organisation.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Canadian private sector privacy legislation provides that the amount of PI that an organisation collects should be limited to what is necessary for the identified purpose. Organisations cannot require individuals to consent to the collection, use or disclosure of PI as a condition for providing a product or service beyond that required to fulfil the explicitly specified and legitimate purpose.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Canadian privacy legislation also provides that, absent any specific legislative requirements to keep the PI for a certain period of time, the PI should be held only as long as is necessary to fulfil its identified purpose, and once it is no longer required to fulfil this purpose, it should be destroyed, erased or made anonymous.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Under PIPEDA, the purpose for which PI is collected must be one that a reasonable person would consider appropriate in the circumstances. Organisations are generally required to identify the purposes for which PI is collected at or before the time of collection. PI must not be used or disclosed for a new or other purpose, except with fresh consent of the individual or as permitted or required by law.

If an organisation wishes to use PI in its possession for a new purpose, it must obtain fresh consent from individuals to use their PI for the newly identified purpose.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Canada does not have a dedicated artificial intelligence (AI) law. There is a recognised need for a framework, but to date, primarily soft law tools have been utilised. In the public sector, the federal government developed the Directive on Automated Decision-Making in 2019, but this applies only to the federal government. It provides for an algorithmic impact assessment that classifies the impact of decisions into particular levels, which then have associated requirements, such as differing levels of notice and explanation, and the potential for a human in the loop.

In the private sector, PIPEDA is due to be updated. The federal government introduced Bill C-11 in 2020, which was intended to update PIPEDA and included several relevant provisions; however, it died when an election was called in 2021. The federal government has not yet reintroduced the bill. The OPC has tried to utilise current data protection laws to address issues specific to AI. In a joint decision relating to Clearview AI, the OPC and their provincial counterparts found that express consent is required to scrape biometric data from the internet for use in a facial recognition tool. In addition, they found that Clearview AI's stated purpose (collecting, using and disclosing personal information to provide a service to law enforcement personnel) was inappropriate and could not be rendered appropriate by consent.

While Canada's private sector data protection laws are currently under some level of review, Quebec has passed Bill 64, which significantly updates their public and private sector data protection laws. The amendments come into effect in stages over the next three years. Effective 22 September 2023, any public body or private organisation that renders a decision based exclusively on automated processing must inform the person concerned of this fact not later than when advising them of the decision itself. On request, the individual is also entitled to know what PI was used and the reasons and principal factors and parameters that led to the decision. Individuals have the right to have the PI utilised correctly and must be given the opportunity to submit observations to a person who is in a position to review the decision.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Canadian privacy legislation requires that organisations implement reasonable technical, physical and administrative safeguards to adequately protect PI against loss or theft and from unauthorised access, disclosure, copying, use or modification, regardless of the format in which it is held. Specific security safeguards are generally not included in legislation, and the onus is on the organisation to ensure that appropriate security safeguards are in place.

In assessing what constitutes 'appropriate security safeguards', consideration must be given to the nature of the PI and the harm that might result from its loss, theft, unauthorised access, disclosure, copying, use or modification. As the sensitivity of the PI increases, so increases the assumed risk of harm, thereby increasing what constitutes an appropriate level of security safeguards.

Where organisations engage service providers to process PI on their behalf, such organisations remain responsible for protecting the PI. They have an obligation to ensure, through contractual or other means, that the service providers are themselves using appropriate security safeguards for the PI.

Certain types of PI, such as those related to health or financial matters, may also be subject to industry-specific legislation that imposes specific security obligations on the owners of PI.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) includes mandatory breach notification requirements. A data breach is the unauthorised access to, or collection, use or disclosure of, PI. If a breach of security safeguards involving

PI poses a real risk of significant harm to individuals, an organisation must:

- report to the Office of the Privacy Commissioner of Canada (OPC);
- notify affected individuals as soon as feasible; and
- notify any government institution or organisation that it believes can reduce or mitigate the risk of harm that could result from the breach.

The report to the OPC must be made in prescribed form and the notice to the affected individuals must contain the information set out in the regulations.

Organisations under PIPEDA are also required to keep records, in prescribed form, of all breaches of security safeguards involving PI under its control, and to provide the Privacy Commissioner with a copy of such records on request. Those records must be kept for at least two years.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) incorporates 10 fair information principles as Schedule 1 to PIPEDA. Organisations are required to implement policies and practices to give effect to those principles, including procedures to protect PI, receive and respond to complaints and inquiries, train staff on those procedures and develop information for the public explaining those procedures. Organisations must use contractual or other means to ensure third-party service providers provide a comparable level of protection of PI.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

PIPEDA, Alberta's Personal Information Protection Act (PIPA AB) and British Columbia's Personal Information Protection Act (PIPA BC) expressly require organisations to appoint an individual who is accountable for ensuring compliance with the organisation's data protection obligations and who may, in turn, delegate some of his or her responsibilities to others. Such individuals are typically referred to as the 'chief privacy officer' or 'privacy officer', although the legislation does not prescribe any particular title. They are generally accountable for an organisation's policies and practices, and they are the designated individual to respond to inquiries, complaints and access requests. There are no express legal criteria, but the privacy commissioners responsible for enforcing PIPEDA, PIPA AB and PIPA BC have issued joint Accountability Guidelines that recommends the privacy officer be a senior individual. Effective 22 September 2022, Quebec's An Act Respecting the Protection of Personal Information in the Private Sector (the Private Sector Act (QC)) provides that the individual with the highest authority in an organisation is deemed the privacy officer by default, but that role may be delegated completely or in part.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Absent a breach of security safeguards or an access request, there is no specific record-keeping requirement for private sector organisations, subject to any industry specific requirements. In addition, certain provincial health-related legislation requires maintaining records in certain circumstances.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Privacy impact assessments are required for federal institutions under the Treasury Board Secretariat Directive on Privacy Impact Assessments. They are generally required if a programme or activity may utilise PI as part of a decision-making process that directly affects individuals, where there are major changes to an existing programme or activities where PI may be used for administrative purposes, and where there are major changes to existing programmes or activities as a result of contracting out or transferring programmes or activities to another level of government or the private sector.

PIPEDA does not explicitly require risk assessments; however, the information required to obtain valid consent implies the need. The OPC has released guidance on obtaining meaningful consent, which indicates that advising individuals of the potential harms that could result from the collection, use or disclosure of their PI is necessary for them to provide valid consent. This, by implication, requires some kind of risk assessment. Further, organisations are required to ensure, through contractual or other means, that PI transferred to service providers for processing receives comparable levels of protection while in the service providers possession. Where this is not possible, organisations should not transfer the PI. This also implies an obligation to perform some kind of risk assessment.

Effective 22 September 2023, the Private Sector Act (QC) will require organisations to conduct a privacy impact assessment (PIA) prior to the acquisition, development or redesign of an information system or electronic service delivery project that involves the collection, use, disclosure, retention or destruction of PI. The PIA must be proportionate to the sensitivity of the information, the purpose for its use, and the amount, distribution and format of the information. Further guidance is forthcoming.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Within the context of the private sector in all jurisdictions other than Quebec, there are no explicit legal obligations in relation to the design of processing operations, such as to apply a privacy-by-design approach or carry out PIAs. However, the OPC has found in certain circumstances particular default settings are required based on individuals' reasonable expectations.

Effective 22 September 2023, the Private Sector Act (QC) will require that organisations offering technological products or services to the public that collect personal information must set any privacy parameters to their highest level of confidentiality by default.

In the context of the public sector, certain of the provincial or territorial privacy enactments require, in certain circumstances, that privacy impact assessments be performed in the context of the design and development of products and services.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Generally, organisations that collect, use or disclose PI do not have a legal obligation to register with a supervisory authority. Organisations that wish to use or disclose PI, without consent, for statistical or scholarly study or research purposes must, however, notify the OPC before such use or disclosure.

Other transparency duties

29 | Are there any other public transparency duties?

Canadian privacy legislation, generally speaking, requires organisations to establish policies and practices detailing how the organisation addresses privacy and related obligations under the various pieces of legislation. While, for the most part, the legislation leaves the exact nature of the policies and practices to the discretion of the organisation, it is now accepted that, at the very least, an organisation must have a public-facing privacy policy.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Organisations are responsible for the PI they collect, use and disclose, even when it is being transferred to third-party service providers for processing. As such, while organisations are, in general, permitted to transfer PI to service providers without consent, they must ensure, through contractual or other means, that a comparable level of protection is afforded to the PI when it is processed by a third party. Moreover, the PI can only be used by a third party for the purposes for which it was originally collected, and organisations must be transparent about their information-handling practices.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The sharing of PI with recipients who are not processors or service providers is considered a disclosure under Canadian privacy laws, including the federal private sector legislation the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA requires that any disclosure be for a purpose that a reasonable person would consider appropriate in the circumstances. Such a disclosure would typically require the consent of the individual, except in limited circumstances such as in compliance with the rules of a court relating to the production of records. In such circumstances, the remaining requirements of the applicable privacy legislation still apply, including the appropriate purpose requirement, and the obligation to limit disclosure to only what is reasonably necessary and to appropriately safeguard the transmission of the PI.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Neither PIPEDA nor any other private sector provincial privacy legislation expressly prohibits the transfer of PI outside of Canada. However, organisations are required to use contractual or other means to provide the PI with a comparable level of protection to that which it would have received in Canada while the PI is outside the jurisdiction. Moreover, the transfer of the PI must only be used for the purposes for which the PI was initially collected and organisations must be transparent about their information handling practices, including notifying individuals whose PI is being processed that, among other things, their data is being sent elsewhere.

Alberta's Personal Information Protection Act (PIPA (AB)) contains statutory requirements for the transfer of PI outside of Canada. Under PIPA (AB) an organisation intending to transfer PI outside of Canada for processing must first provide notice to individuals of its policy and procedures addressing such transfers, and contact information of its representative who can respond to questions regarding such activities. The organisation should also notify the individuals concerned that transfers of data may be made.

Effective 22 September 2023, both Quebec's public sector and private sector privacy legislation will require organisations and public bodies to conduct a privacy impact assessment prior to transferring PI outside of Quebec, and will limit the transfer of PI outside of Quebec to jurisdictions that have privacy protection legislation in place equivalent to that which exists in Quebec.

Alberta and British Columbia restrict the transfer of public sector PI outside of Canada and, in some instances, outside of the province. With limited exceptions, consent of the affected individuals being one, Nova Scotia prohibits government institutions and Crown agents, as well as their service providers, from transferring PI outside of Canada. Nova Scotia and Newfoundland and Labrador restrict the transfer of health PI outside each respective province.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

To the extent that transfers outside of Canada are subject to obligations, such obligations apply equally to transfer to service providers and onward transfers.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no requirement for a copy of personal information to be maintained in Canada; however, some public sector laws impose restrictions on the transfer of PI outside the province or Canada. Effective 22 September 2023, Quebec's public sector and private sector privacy legislation will require organisations and public bodies to conduct a privacy impact assessment prior to transferring PI outside of Quebec, and will limit the transfer of PI outside of Quebec to jurisdictions that have privacy protection legislation in place equivalent to that which exists in Quebec.

Alberta and British Columbia restrict the transfer of public sector PI outside of Canada and, in some instances, outside of the province. With limited exceptions, consent of the affected individuals being one, Nova Scotia prohibits government institutions and Crown agents, as well as their service providers, from transferring PI outside of Canada.

Nova Scotia and Newfoundland and Labrador restrict the transfer of health PI outside each respective province.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under Canadian privacy legislation, organisations must, upon request and subject to limited exemptions, inform individuals of the existence, use and disclosure of an individual's PI, and must give them access to that information, including a listing of the third-party organisations with whom the information has been shared.

The right of access does not oblige an organisation to provide copies of PI records; rather, it requires the provision of access, which may include viewing the records at an organisation's offices. Generally, an individual's request must be sufficiently specific as to allow an organisation to identify the records.

Under Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) and British Columbia's Personal Information Protection Act (PIPA (BC)), an organisation must respond to an access request not later than 30 days after receipt of the request. Under Alberta's Personal Information Protection Act (PIPA (AB)), an organisation must respond to an access request not later than 45 days after receipt of the request. Each of the Acts contains provisions enabling an organisation, in certain circumstances, to extend the prescribed time frame for a response by another 30 days. While the circumstances vary slightly depending on the legislation, one common example is where additional time is required to undertake consultations with another organisation prior to responding to the request.

Under Quebec's An Act Respecting the Protection of Personal Information in the Private Sector (the Private Sector Act (QC)), an organisation must respond to an access request no later than 30 days after the date of the receipt of the request. Failure to respond within this time frame is deemed to be a refusal to grant the request.

Under PIPEDA, PIPA (BC) and PIPA (AB) access must be granted at minimal or no cost to the individual, and must make the information available in a form that is generally understandable.

Under the Private Sector Act (QC) access must be provided free of charge. However, a reasonable charge may be required from a person requesting a transcription, reproduction or transmission of the PI in question.

The exemptions to the right of access vary among legislation and need to be carefully considered. Examples of the statutory exemptions include, but are not limited to, information subject to solicitor–client or litigation privilege, confidential commercial information, information about another individual, information that relates to national security matters and information generated in a formal dispute resolution process.

Other rights

36 | Do individuals have other substantive rights?

Generally, individuals have the following rights in relation to PI held by organisations:

- to gain access to PI, including whether and what type of PI is held and a general account of its use and disclosure;
- to amend PI if it is inaccurate or incomplete;
- to acquire information as to an organisations' PI handling practices and policies without unreasonable effort, including that PI is made available to related organisations, such as subsidiaries;
- to withdraw consent at any time, subject to any contractual or legal restrictions, reasonable notice (the individual must be informed of the implications of withdrawal of consent); and
- to make a complaint to the relevant privacy authority (prior to doing so, individuals should address privacy issues with the designated privacy officer or equivalent within the organisation who is accountable for the organisation's compliance).

Whether there is a General Data Protection Regulation (GDPR)-type 'right of erasure' of PI, it is currently unsettled in common law areas of Canada. Quebec, which recently passed an amendment to their privacy laws, has granted three new rights. Effective 22 September 2023, Quebec residents will have the right to be informed of, and object to, automated decision-making and the right to restrict the dissemination (a more limited form of the right to be forgotten found in the GDPR). Effective 22 September 2024, Quebec residents will have the right to data portability.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

There is no private right of action provided in the Personal Information Protection and Electronic Documents Act; however, a complainant can apply to the courts for a hearing de novo once a report has been issued by the Office of the Privacy Commissioner of Canada. While the courts have the power to award damages to the complainant, typically these awards are nominal.

Further, individuals affected by breaches of the law and seeking monetary damages or compensation can seek redress through private legal action. Such individuals may be entitled to monetary damages or compensation for wrongful acts either under the common law or pursuant to those statutes that provide for a private right of action. As a rule, individuals must establish that they suffered actual damage as a direct result of negligent actions in order to be successful; however, some statutory and common law invasion of privacy torts do not require proof of damages.

Finally, effective 22 September 2023 the Private Sector Act (QC) will provide a private right of action.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights of individuals affected by breaches of the law and seeking monetary damages or compensation are exercisable primarily through the judicial system. Typically, the civil penalties imposed by supervisory authorities are not paid directly to aggrieved individuals, but there are exceptions.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Under Canadian privacy legislation, there are both mandatory and discretionary exceptions to the access, consent, use and disclosure of PI. The type of exceptions will depend upon the PI at issue, the jurisdiction and whether an organisation is in the public or private sector. The specific applicable legislation ought to be consulted to carefully determine if any applicable exceptions exist. Some common types of

exceptions centre around PI related to an investigation, national security, artistic or literary purposes, study or research purposes, or protecting the health or safety of individuals.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Canada does not have specific legislation regulating 'cookies'. Rather, cookies, are subject to Canada's Anti-Spam Legislation (CASL) and privacy laws.

Under CASL, express consent must be obtained prior to installing any kind of computer program on another's computer in the course of commercial activity; however, an exception is provided with respect to cookies and certain other computer programs. Where the person seeking consent is identified, individuals are deemed to have expressly consented under CASL if their conduct is such that it is reasonable to believe they, through their actions, have consented to the installation.

Under privacy laws, consent may be obtained through express or implied means. To the extent that the PI is sensitive in nature, express consent is required. If the PI is non-sensitive in nature, implied (or opt-out) consent is acceptable for the purposes of online behavioural advertising, provided that:

- individuals are made aware of the purposes for the practice in a manner that is clear and understandable;
- individuals are informed of the purposes at or before the time of collection, and are provided with information about the various parties involved in online behavioural advertising;
- individuals are able to easily opt out of the practice at or before the time the information is collected;
- the opt-out takes effect immediately and is persistent;
- the information collected and used is limited, to the extent practicable, to non-sensitive information; and
- information collected and used is destroyed or effectively anonymised as soon as possible.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Unless an exception or exemption applies, it is unlawful under CASL to send, or cause or permit to be sent, a commercial electronic message (defined broadly to include text, sound, voice or image messages) to an electronic address, unless the recipient has provided express or implied consent. The message must comply with the prescribed form and content requirements, including containing an unsubscribe mechanism.

Targeted advertising

42 | Are there any rules on targeted online advertising?

The Office of the Privacy Commissioner of Canada has taken the position that because of the scope, scale and nature of information collected, as well as tools available for analysis, information collected for targeted online advertising will generally constitute PI. As such, privacy laws apply and consent is required through express or implied means. To the extent that the PI is sensitive in nature, express consent is required. If the PI is non-sensitive in nature, implied (or opt-out) consent is acceptable for the purposes of online behavioural advertising, provided that:

- individuals are made aware of the purposes for the practice in a manner that is clear and understandable;
- individuals are informed of the purposes at or before the time of collection, and are provided with information about the various parties involved in online behavioural advertising;
- individuals are able to easily opt out of the practice at or before the time the information is collected;
- the opt-out takes effect immediately and is persistent;
- the information collected and used is limited, to the extent practicable, to non-sensitive information; and
- information collected and used is destroyed or effectively anonymised as soon as possible.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Privacy legislation generally states that the more sensitive the PI, the greater the security safeguards required to protect it. It is up to an organisation to determine what is appropriate in the particular circumstances. The Office of the Privacy Commissioner of Canada (OPC), which oversees Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA), has released guidance that states while some information (health and financial, etc) is always considered sensitive and subject to more stringent protections, any PI could be considered sensitive depending on the context.

In addition, the type of consent required will depend on the sensitivity of the PI being collected, used or disclosed. Sensitive PI will generally require express consent.

Finally, the vast majority of provinces have health legislation that applies specifically to entities that fit within the definition of 'custodians' or 'trustees' and have stricter and more specific standards of security safeguards for health PI.

Profiling

44 | Are there any rules regarding individual profiling?

The OPC has updated their policy position on online behavioural advertising (OBA). The OPC has taken the position that they will generally consider information collected for the purpose of OBA to be PI given that the purpose is to create profiles of individuals to permit serving targeted ads, among other things. As such, PIPEDA will apply. The OPC has determined that OBA may be considered an appropriate purpose for the collection, use and disclosure of PI under PIPEDA, but it cannot be considered a term or condition for use of the Internet generally. Consent, limitation and other fair information principles found in PIPEDA will apply.

Effective 22 September 2023, Quebec's An Act Respecting the Protection of Personal Information in the Private Sector will include an obligation to advise individuals of the use of technology that allows them to be identified, located or profiled, and of the means available to activate those functions.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There are no specific rules or legislation that governs the processing of the PI through cloud computing services. However, the OPC, in conjunction with the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, has developed guidance to assist organisations in understanding the privacy implications and responsibilities associated with the use of cloud computing services and provide suggestions to address those concerns.

UPDATE AND TRENDS

Key developments of the past year

46 Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Privacy law reform remains a hot topic in Canadian data protection. Canada's current federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), was enacted in 2001 and has, for some time, been considered in need of substantive reform. On 16 June 2022, the federal government tabled Bill C-27, the Digital Charter Implementation Act 2022. If passed, this Act would establish a new Canadian federal privacy law for the private sector as well as legislation aimed at regulating artificial intelligence. It would do so by creating the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act (PIDPTA) and the Artificial Intelligence and Data Act (AIDA).

The CPPA will repeal and replace the privacy sections of PIPEDA, leaving only the Electronic Documents Act. The PIDPTA will establish the Personal Information and Data Protection Tribunal (the Tribunal), which will have the power to impose penalties as well as hear appeals of certain decisions made by the Privacy Commissioner. The AIDA will regulate international and interprovincial trade and commerce in artificial intelligence systems (AI Systems) by, among other things, creating a new Artificial Intelligence and Data Commissioner and imposing obligations such as impact assessments enforced by orders and administrative monetary penalties.

If Bill C-27 were to pass in its present form, the CPPA will introduce a number of changes. Among other things, it will:

- define de-identified and anonymised data, and clarify that de-identified data is still PI except in certain circumstances;
- codify an express obligation to implement and maintain a privacy management programme with prescribed components;
- modernise consent rules to ensure that individuals have the plain language information necessary to make meaningful choices about the use of their PI, as well as introduce several new exceptions to the need for consent, such as for business activities or activities that a business has a legitimate interest in. Neither exception can be used where PI is collected or used for the purpose of influencing individuals' behaviour or decisions;
- give individuals the right to direct the transfer of their personal information and, in most cases, permit individuals to withdraw consent for the use of their PI; and
- give individuals the ability to demand that their PI be disposed of if they have withdrawn their consent or the PI is no longer necessary for the provision of a product or service requested by the individual. The CPPA allows organisations to refuse to dispose of PI in certain circumstances.

Also, if Bill C-27 were to pass in its present form, the CPPA will grant the Privacy Commissioner broad order-making powers, and, in addition, the ability to recommend to the Tribunal that it impose significant monetary penalties on those found to have contravened the CPPA. The CPPA includes administrative monetary penalties (AMPs) of up to the greater of C$10 million or 3 per cent of an organisation's gross annual revenue in the prior financial year. For more serious violations, penalties are up to the greater of C$25 million or 5 per cent of an organisation's gross annual revenue in the prior financial year, if found guilty of an indictable offence.

If passed, the AIDA will be the first stand-alone law regulating artificial intelligence in Canada, though much of its impact will come from regulations that have yet to be released. For example, the AIDA specifies that the following things must be done 'in accordance with the regulations':

- establishing measures with respect to the manner in which data processed or made available for use is anonymised;
- establishing measures for the use or management of anonymised data;
- assessments with respect to whether an AI System is a 'high-impact system' (a term that itself is defined by reference to the criteria established in regulations);
- establishing measures to identify, assess and mitigate the risks of harm or biased output;
- establishing measures to monitor compliance with the mitigation measures;
- general record-keeping describing the above noted measures and the reasons supporting assessments regarding the nature of the AI System; and
- providing prescribed plain language information about the AI System on a publicly available website.

AI System is broadly defined to include any 'technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.'

The AIDA provides for the imposition of AMPs where a person has committed a violation, but the details are left to the regulations, including both what constitutes a violation and the amount of the penalties. The AIDA also creates several offences. The punishment for an offence can range from a fine of not more than the greater of C$5 million and 2 per cent of gross global revenues in the prior financial year up to the greater of C$25 million and 5 per cent of gross global revenues in the previous year, depending on the section of the AIDA contravened and other factors. The more serious offences also include the possibility of a term of imprisonment.

In addition to the Canadian federal government, privacy law reform or introduction has occurred or been considered in the provinces of Quebec, British Columbia and Ontario.

The Province of Quebec took significant steps toward modernising its current privacy laws when it signed into law Bill 64, An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information. The Bill significantly amends the current Act Respecting the Protection of Personal Information in the Private Sector (the Private Sector Act (QC)), as well as other legislation. The changes to the Private Sector Act (QC) will come into force in three stages. Some provisions, such as mandatory breach reporting, will come into effect on 22 September 2022. The majority of the amendments will come into force on 22 September 2023. Finally, the new right to data portability will come into effect on 22 September 2024.

Some of the most significant changes include new individual rights and new enforcement mechanisms. The enforcement mechanisms now include penal offences, administrative monetary penalties and a private right of action. The new individual rights include a version of the right to be forgotten, the right to data portability, the right to be informed of and object to automated decision-making and the right to request information about data processing. Penal offences can result in a penalty of up to C$25 million or 4 per cent of worldwide turnover in the preceding year, whereas administrative monetary penalties can result in a penalty of up to C$10 million or 2 per cent of worldwide turnover in the preceding year.

In British Columbia, the provincial government continues to review its Personal Information Protection Act (PIPA (BC)). A special committee, struck in February 2020, issued its final report on the modernisation of British Columbia's private sector law on 6 December 2021. The

report included 34 recommendations, including aligning PIPA (BC) with changing federal provincial and international privacy regimes, including the European Union's General Data Protection Regulation. Other recommendations included addressing pseudonymised and anonymised information, automated decision-making processes, and stronger auditing and enforcement powers for the Office of the Information and Privacy Commissioner. Which of these recommendations will be acted upon remains to be seen.

In the province of Ontario, the Ministry of Government and Consumer Services released a white paper entitled 'Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy'. This white paper outlined proposals to address some gaps that result from the constitutional division of powers in Canada, as well as how outdated privacy laws have become. It was intended to facilitate dialogue to assist the government in determining whether Ontario should proceed with its own privacy legislation and, if so, how such legislation would be structured. The white paper noted that Bill C-11 had specific weaknesses, which Ontario wanted to address. When Bill C-11 died on the order paper with the announcement of the 2021 federal election, the Information and Privacy Commissioner of Ontario (ICPO) urged the government of Ontario to proceed with a provincial law regardless of what happens federally.

Ontario also introduced and passed Bill 88. Schedule 1 to Bill 88 enacts the Digital Platform Workers' Rights Act 2022, which establishes certain rights for workers who perform digital platform work. Digital platform work is defined to mean the provision of for-payment ride-shares and delivery, courier or other prescribed services by workers offered assignments using a digital platform. These types of work environments have given rise to incredibly privacy-invasive ways of supervising and measuring the performance of workers. The Bill also amends other legislation, like the Employment Standards Act. Such amendments require employers with 25 or more employees to tell their workers if, how and in what circumstances they are being monitored electronically. The ICPO noted that while this Bill was a laudable first step, it did not go far enough by imposing transparency obligations without any restrictions on workplace surveillance, such as an obligation to use surveillance only for fair and appropriate purposes and only as reasonably necessary.

B Douglas Tait
bdt@tdslaw.com

Kendall N Dyck
knd@tdslaw.com

Suite 1700
242 Hargrave Street
Winnipeg
Manitoba R3C 0V1
Canada
Tel: +1 204 957 1930
www.tdslaw.com

Chile

Claudio Magliona, Nicolás Yuraszeck and Carlos Araya

Magliona Abogados

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The legal framework for data protection can be found in article 19 No. 4 of the Political Constitution of the Republic of Chile, which guarantees that the processing and protection of personal data shall be carried out in the manner and under the conditions laid down by law. In addition, Chile has a dedicated data protection law, Law No. 19,628 on Privacy Protection, which was published in the Official Gazette on 28 August 1999 (the Law). The current Law is not based on any international instrument on privacy or data protection in force (such as the Organization for Economic Cooperation and Development guidelines, Directive 95/46/EC, EU General Data Protection Regulation or the European Convention on Human Rights and Fundamental Freedoms).

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

There is no special data protection authority in Chile; data protection overseeing is addressed by general courts with general powers. A summary procedure is established by law if the person responsible for the personal data registry or bank fails to respond to a request for access, modification, elimination 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.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Currently, there is no data protection authority in Chile. A bill has been discussed in Congress that will reform the whole data protection environment in the country and will create the first data protection authority in Chile.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Yes. Breaches of data protection caused by improper processing of data may eventually lead to fines determined by the Law (ranging from 57,557 Chilean pesos to 575,570 Chilean pesos, or from 575,570 Chilean pesos to 2,877,850 Chilean pesos). Fines are viewed and determined in a summary procedure.

The Law establishes a general rule under which both non-monetary and monetary damages that result from wilful misconduct or negligence in the processing of personal data shall be compensated. In those cases, the amount of compensation shall be established reasonably by a civil judge, considering the circumstances of the case and the relevance of the facts.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Currently, there is no personal data authority in Chile. Therefore, at present, the holder of personal data could not appeal a decision of the personal data authority. Notwithstanding this, the courts of appeal could hear claims regarding personal data. In the case of infringement of the constitutional right to the protection of personal data, the affected party may resort to the court of appeal through an appeal for protection. The same applies in the second instance in the case of an infringement in the processing of personal data according to Chilean law.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Law No. 19,628 on Privacy Protection (the Law) applies to both private and public sector organisations and agencies. However, regarding public sector organisations, there are some special rules for the consent of the subject: personal data about sentences for felonies, administrative sanctions or disciplinary failures and the records of personal data banks in government agencies.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Data Protection Law does not cover interception of communications or monitoring and surveillance of individuals. Both matters are regulated by:

- Law No. 19,223 (the Computer Crime Law);
- article 161-A, 369-ter, 411-octies of the Penal Code; and
- articles 222 to 226 of the Criminal Code of Procedure.

The Data Protection Law does cover electronic marketing, in the sense of establishing that no authorisation is required to make electronic marketing when the information comes from sources available to the public (registries or collection of personal data, public or private, with unrestricted or unreserved access to the requesters).

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Numerous laws address privacy issues, for example:

- Law No. 19,223 (the Computer Crime Law);
- article 161-A, 369-ter, 411-octies of the Penal Code;
- articles 222 to 226 of the Criminal Code of Procedure;
- Law No. 20,584, which contains provisions regarding the privacy of medical records along with Law No. 19,628, which contains provisions stipulating that a doctor's prescriptions and laboratory analyses or exams and services related to health are confidential;
- Law No. 19,496, which contains provisions regarding credit information along with the same Law No. 19,628, which contains provisions about personal data related to obligations of an economic, financial, banking or commercial character;
- Law No. 18,290, which contains provisions regarding the privacy of a driver's information;
- Law No. 19,799 regarding electronic signatures, which contains the right to privacy of the holder of an electronic signature; and
- article 154-bis of the Labour Code, which establishes that the employer shall keep confidential all the information and private data of the worker to which he or she has to access on the occasion of the employment relationship.

Also, article 5 of the Labour Code establishes that the exercise of powers granted to the employer by law is limited by respect for the constitutional guarantees of the workers, especially when they may affect their privacy, private life or honour.

PI formats

9 | What categories and types of PI are covered by the law?

All formats of personal data are covered by the Law, regardless of whether they are in electronic records or manual files.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Law does not contain an explicit provision in this respect; however, any use of the data will require consent or authorisation of the holder or subject of the personal data, if it is not subject to the exceptions mentioned in this document (transfer is a kind of personal data processing, thus, all the data privacy rules shall apply, including the consent requirement).

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Yes, all processing of PI is covered. 'Data processing' is broadly defined in the Law as any operation or set of technical operations or procedures, automated or not, that makes it possible to collect, store, record, organise, prepare, select, extract, match, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use it in any form.

There is no distinction made between those who control or own PI and those who provide PI processing services to owners. The Law only refers to the 'person responsible for a data registry or a bank', which means any private legal entity or individual, or government agency, that has the authority to implement the decisions related to the processing of personal data. Therefore, there are no different duties for owners, controllers or processors. However, government agencies can only process data regarding matters within their respective legal authority and subject to the rules set out in the Law.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes, Law No. 19,628 on Privacy Protection (the Law) provides that any person may process personal data if he or she meets the following requisites:

- the processing of personal data is authorised by one of the three following means:
  - the Law;
  - another legal provision; or
  - the subject of the personal data (the individual to whom the personal data refers) specifically consents thereto;
- the rights granted by the Law to the subjects of the personal data are observed (right to know, right of access, and right to rectify, eliminate and block);
- the purpose of the personal data processing is permitted by the Chilean legal system;
- full exercise of the fundamental rights (rights established in the Political Constitution of Chile) of the subjects of the personal data is respected; and
- the authorisation granted by the subject related to the processing of his or her personal data must comply with the following requirements to be valid:
  - it must be definitely stated;
  - the person authorising must be properly informed about the purpose of the storage of his or her personal data and its possible communication to the public;
  - it must be stated in writing;
  - the personal data must be used only for the purposes for which it has been collected unless it comes or has been collected from sources available to the public; and
  - the information must be exact, updated and respond truthfully to the real situation of the subject of the data.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Yes. The Law imposes more stringent rules concerning sensitive data, which is defined as that which refers to the physical or moral characteristics of persons or facts or circumstances of their private life or intimacy, such as personal habits, racial origin, ideologies and political opinions, beliefs or religious convictions, conditions of physical or mental health and sex life.

The sensitive data may not be subject to processing unless the law so authorises, there is consent from the subject or it is necessary data for the determination or granting of health benefits for the subjects.

The Law also contains special provisions that apply to PI included in an individual's economic, financial, banking or commercial information and its communication.

Conditions of physical or mental health are considered sensitive data. The sensitive data may not be subject to processing unless it is necessary for the determination or granting of health benefits. Thus, health data may be processed for the determination or granting of health benefits, in case the healthcare provider does not gain the authorisation of the individual.

Doctors' prescriptions and laboratory analyses or exams and services related to health are confidential. Such content can only be revealed or copied with the express consent of the patient, granted in writing.

The aforementioned does not prevent pharmacies from publishing, for statistical purposes, the sales of pharmaceutical products of any nature, including the name and amount thereof. In no case shall the information provided by the pharmacies state the name of the patients who present the prescriptions, the name of the medical doctors that issued them or data that serves to identify them.

Finally, financial data may not be processed in the following cases:

- after five years since the respective obligation was enforceable;
- in the case of debts incurred during a period of unemployment;
- in the case of data relating to obligations that have been paid or extinguished by other legal means; and
- in the case of debts of electricity, water, telephone, gas and highways.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

No, Law No. 19,628 on Privacy Protection (the Law) does not require owners of PI to notify individuals whose data they hold. The Law requires authorisation, not notice. The authorisation must be definitely stated, stated in writing and informed about the purpose of the storage of his or her personal data and communication to the public.

Exemptions from transparency obligations

15 | When is notice not required?

Even though notice is not required, authorisation is still required. Such authorisation is not required when:

- the personal data is processed by public organisations regarding matters within their respective legal authority and subject to the rules set out in the Law;
- the personal data is originated or is collected from sources available to the public when such data is:
  - of an economic, financial, banking or commercial nature;
  - contained in listings relating to a class of persons and is limited to indicating information such as the fact of belonging to such a group, the person's profession or business activity, educational degrees and address or date of birth; or
  - necessary for direct response commercial communications or direct sale of goods and services; or
- the personal data is processed by private legal entities for their exclusive use, or the exclusive use of their associates and entities that are affiliated with them, for statistical or rate-setting purposes or other purposes of general benefit to such private legal entities.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes. The Law requires that the information must be exact, updated and respond truthfully to the real situation of the subject of the data. The Law also establishes that personal data shall be blocked if its accuracy cannot be established or its validity is doubtful and its cancellation is not appropriate.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Yes, the Law restricts the collection of sensitive data. Sensitive data cannot be processed, except when authorised by law, with the consent of the owner or as necessary for the determination or granting of health benefits to their owners.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Yes, the Law restricts the length of time PI may be held. Personal data must be eliminated or cancelled when there are no legal grounds for its storage or when the data has expired.

In addition, personal data related to the obligations of an economic, financial, banking or commercial nature, and relating to an identified or identifiable individual, may not be communicated five years after the respective obligation began.

Regarding government agencies that process personal data about sentences for felonies, administrative infractions or disciplinary failures, they may not communicate them after the statute of limitations applicable to the criminal or administrative action, sanction or penalty has been subject to a statute of limitations, or after the sanction or penalty has been served.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes. The Law expressly foresees that personal data must be used only for the purposes for which it has been collected, and those purposes must be permitted by the Chilean legal system. In any case, the information must be exact, updated and respond truthfully to the real situation of the subject of the data.

The limit of the finality principle is given by the purposes permitted by the Chilean legal system and according to the Law's provisions. Purposes beyond the scope of the Law or the Chilean legal system are not allowed.

There is one exception to the aforesaid principle, and it comes when the data has been collected from sources available to the public.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

At present, there is no express rule regulating this matter. The only thing that is stated is that the person in charge of the registry or personal data bank may establish an automated procedure for the transmission of personal data, provided that the automated transmission procedure, the rights of the data subjects and the transmission is related to the tasks and purposes of the participating organisations.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Law No. 19,628 on Privacy Protection (the Law) Law does not impose any type of security measures that data owners and entities must take concerning PI. Instead, it mentions that the person responsible for the registries or bases where personal data is stored after its collection shall take care of them with due diligence, assuming responsibility for damages. However, there are specific rules regarding banks and the data of their clients and their wire transfers, in which encryption is mandatory.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

No. The Law does not impose any obligations to notify the regulator or individuals of security breaches, because currently in Chile there is no data regulator.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

At present, Law No. 19,628 on Privacy Protection does not require internal controls for personal data processors; it only states that the person responsible for the records or bases where data is stored after their collection must take care of them with due care.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

No. There is no data protection officer in Chile.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

No, owners or processors of PI are not required to maintain any internal records or establish internal processes or documentation.

However, regarding personal data processing by government agencies, the Service of Civil Registration and Identification shall keep a record of personal data banks managed by such agencies.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

At present, there is no obligation in this matter.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

No, currently there are no obligations in relation to new processing operations.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

No. There are no registration requirements for data-processing activities in Chile. However, the Service of Civil Registration and Identification shall keep a record of personal data banks managed by government agencies.

Other transparency duties

29 | Are there any other public transparency duties?

No, currently the Law No. 19,628 on Privacy Protection does not contemplate any public transparency duty.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

At present, Law No. 19,628 on Privacy Protection (the Law) does not contain a specific provision in this respect. However, considering that transfer of data is deemed as data processing according to the Law, it follows that it will require authorisation of the individual unless there are exceptions contemplated by the Law and the authorisation is not subject to one of the following exceptions:

- the personal data is processed by public organisations regarding matters within their respective legal authority and subject to the rules set out in the Law;
- the personal data is originated or is collected from sources available to the public when such data:
  - is of an economic, financial, banking or commercial nature;
  - is contained in listings relating to a class of persons and is limited to indicating information such as the fact of belonging

to such a group, the person's profession or business activity, educational degrees and address or date of birth; or
- is necessary for direct response commercial communications or direct sale of goods and services; or

- the personal data is processed by private legal entities for their exclusive use, or the exclusive use of their associates and entities that are affiliated with them, for statistical or rate-setting purposes or other purposes of general benefit to such private legal entities.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

There are no further restrictions on the disclosure of PI to other recipients other than the authorisation of the individual (if not subject to the exceptions aforementioned), the rights of the individual are safeguarded and the transmission is related to the tasks and purposes of the participating agencies.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The Law does not contain a specific provision in this respect. However, the transfer of PI outside the jurisdiction is considered as data processing and will require authorisation.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The Law does not contain a specific provision in this respect. However, any use of the data will require authorisation, if it is not subject to the exceptions mentioned earlier.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

At present, this issue is not legally regulated in Chile.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes. According to Law No. 19,628 on Privacy Protection (the Law), the individual has the right to demand information about data about him or herself, its origin and addressee, the purpose of the storage and the identification of the persons or agencies to whom his or her data is regularly transmitted. Notwithstanding the aforesaid, no information may be requested when it prevents or hinders proper compliance with the supervisory functions of the government agency requested or if it affects the confidentiality or secrecy established in legal or regulatory provisions, the security of the nation or the national interest.

To exercise the right to access, the data subject must address the person responsible for the data registry or bank claiming his or her right to access his or her data. This right to access may refer to:
- the origins of the data (how this data was collected);
- the addressee of the data;
- the purpose of the storage of the data; and
- the identification of the persons or agencies to whom his or her data is regularly transmitted.

The information of personal data shall be absolutely free of charge. This right to access cannot be limited through any act or agreement, except for the previous paragraph (government agency, the security of the nation or national interest). If the person responsible for the personal data registry or bank fails to respond to a request within two business days or refuses a request on grounds other than the security of the nation or the national interest, the subject of the personal data shall have the right to attend before the civil court with jurisdiction over the domicile of the party responsible for the data registry or bank requesting protection to his or her right of access.

Other rights

36 | Do individuals have other substantive rights?

Yes. In addition to the right to information or access, the Law also provides individuals with the following rights:
- the right of modification: if the personal data is erroneous, inexact, equivocal or incomplete, and such situation has been evidenced, the subject shall have the right to have it amended;
- the right of blocking: to request the blocking of personal data when the individual has voluntarily provided his or her personal data or it is used for commercial communications and the subject does not want to continue to appear in the respective registry, either definitively or temporarily;
- the right of cancellation or elimination: notwithstanding legal exceptions, the subject may also demand that data be eliminated if its storage lacks legal grounds or if it has expired, when the subject has voluntarily provided his or her personal data, it is used for commercial communications or he or she does not want it to continue appearing in the respective registry, either definitively or temporarily;
- the right to free copy: the information, modification or elimination of personal data shall be absolutely free of charge, and a copy of the pertinent part of the registry that has been changed shall also be provided at the subject's request. If new modifications or eliminations of data are made, the subject may obtain a copy of the updated registry without cost, as long as at least six months have passed since the last time he or she made use of this right; and
- the right of opposition: the subject may oppose the use of his or her personal data for purposes of advertising, market research or opinion polls.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The Law establishes a general rule under which both non-monetary and monetary damages that result from wilful misconduct or negligence in the processing of personal data shall be compensated, notwithstanding its proceeding to eliminate, modify or block the data as required by the subject or, if applicable, as ordered by the court.

According to Chilean legislation, actual damage is required to be entitled to monetary damages or compensation.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Yes, these rights are exercisable through the judicial system through a summary procedure established by law, if the person responsible for the personal data registry or data bank fails to respond within two business days to a request of access, modification, elimination or blocking of personal data, or refuses a request on grounds other than the security of the nation or the national interest.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Yes. No modification, cancellation or blocking of personal data may be requested when it prevents or hinders proper compliance with the supervisory functions of the government agency to which the request is made or if it affects the confidentiality or secrecy established in legal or regulatory provisions, the security of the nation or the national interest.

Also, Law No. 19,628 on Privacy Protection provides that the modification, cancellation or blocking of personal data stored by legal mandate may not be requested, except for cases contemplated in the respective law.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Law No. 19,628 on Privacy Protection (the Law) does not contain a specific provision in this respect. However, 'cookies' are deemed as data processing according to the Law, hence will require the authorisation of the individual, unless there are exceptions contemplated by the Law, if not subject to the following exceptions:

- the personal data is processed by public organisations regarding matters within their respective legal authority and subject to the rules set out in the Law;
- the personal data is originated or is collected from sources available to the public when such data:
  - is of an economic, financial, banking or commercial nature;
  - is contained in listings relating to a class of persons and is limited to indicating information such as the fact of belonging to such a group, the person's profession or business activity, educational degrees and address or date of birth; or
  - is necessary for direct response commercial communications or direct sale of goods and services; or
- the personal data is processed by private legal entities for their exclusive use, or the exclusive use of their associates and entities that are affiliated with them, for statistical or rate-setting purposes or other purposes of general benefit to such private legal entities.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Law covers electronic marketing in the sense of establishing that no authorisation is required for electronic marketing when the information comes from sources available to the public and it is required for direct response to commercial communications or marketing, or direct sale of goods or services. Though, any individual may require that his or her information be deleted in this case, either permanently or temporarily.

Also, Law No. 19,496 on the Protection of Consumer Rights contains a provision regarding marketing by email (spam). In that case, every promotional or advertising communication sent by email must indicate the subject of what it is, the identification of the sender and a valid email address to which the recipient can request 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 shall indicate an expedited way that the addressees may request the suspension thereof.

Targeted advertising

42 | Are there any rules on targeted online advertising?

At the present, there are no regulations governing this matter.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Yes. The Law imposes more stringent rules concerning sensitive data, which is defined as that which refers to the physical or moral characteristics of persons or facts or circumstances of their private life or intimacy, such as personal habits, racial origin, ideologies and political opinions, beliefs or religious convictions, conditions of physical or mental health and sex life.

The sensitive data may not be subject to processing unless the law so authorises, there is consent from the subject or it is necessary data for the determination or granting of health benefits for the subjects.

The Law also contains special provisions that apply to PI included in an individual's economic, financial, banking or commercial information and its communication.

Conditions of physical or mental health are considered sensitive data. The sensitive data may not be subject to processing unless it is necessary for the determination or granting of health benefits. Thus, health data may be processed for the determination or granting of health benefits, in case the healthcare provider does not gain the authorisation of the individual.

Doctors' prescriptions and laboratory analyses or exams and services related to health are confidential. Such content can only be revealed or copied with the express consent of the patient, granted in writing.

The aforementioned does not prevent pharmacies from publishing, for statistical purposes, the sales of pharmaceutical products of any nature, including the name and amount thereof. In no case shall the information provided by the pharmacies state the name of the patients who present the prescriptions, the name of the medical doctors that issued them or data that serves to identify them.

Finally, financial data may not be processed in the following cases:

- after five years since the respective obligation was enforceable;
- in the case of debts incurred during a period of unemployment;
- in the case of data relating to obligations that have been paid or extinguished by other legal means; and
- in the case of debts of electricity, water, telephone, gas and highways.

Profiling

44 | Are there any rules regarding individual profiling?

At the present, there are no specific rules regarding individual profiling in Chile.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There are no rules or regulatory guidance regarding the use of cloud computing services. Currently, the Law does not contain a specific provision regarding cloud providers; however, the activity of cloud providers may be considered as data processing. Data processing is defined as any operation or set of technical operations or procedures, automated or not, that makes it possible to collect, store, record, organise, prepare, select, extract, match, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use it in any form.

For data processing, it is necessary to comply with the provisions contained in the Law, especially those regarding the authorisation or consent of the individual, the finality principle (personal data must be used only for the purposes for which they have been collected, and those purposes should be permitted by the Chilean legal system) and informing about the potential public communication of the data.

A failure to comply with those provisions (eg, absence of consent of the individual) represents a serious risk and is given a fine, as well as the high risk of litigation (fines are viewed and determined in a summary procedure). Also, the Law establishes a general rule under which both non-monetary and monetary damages that result from improper processing of personal data shall be compensated.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

There is a bill that seeks to amend the current legislation on personal data, updating it and adapting it with Organization for Economic Cooperation and Development standards and the EU General Data Protection Regulation. The bill is still in the first constitutional stage in Congress.

MAGLIONA ABOGADOS

Claudio Magliona
cmagliona@magliona.cl

Nicolás Yuraszeck
nyuraszeck@magliona.cl

Carlos Araya
caraya@magliona.cl

Av. Andrés Bello 2687, 24th floor
Las Condes
Santiago
Chile
Tel: +56 2 3210 0030
www.magliona.cl

China

Gabriela Kennedy and Joshua T K Woo
Mayer Brown

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

In China, rules relating to PI protection and data security are part of a complex framework and are found across various laws and regulations. The Personal Information Protection Law (PIPL), which came into effect on 1 November 2021, works together with China's existing Cybersecurity Law (CSL) and Data Security Law (DSL) to establish a broader framework governing cybersecurity and data privacy protection in China.

The CSL came into operation on 1 June 2017 and was the nation's first comprehensive legislation covering both data privacy and cybersecurity. The CSL sets out a high-level framework regulating the collection, storage, transmission and use of PI by critical information infrastructure (CII) operators and network operators in China.

The DSL, which came into effect on 1 September 2021, regulates the processing of data (including PI), both in an electronic and a non-electronic format. The primary purpose of the DSL is to regulate data processing activities that may impact national security, in particular 'important data' and 'national core data'.

The PIPL, which came into effect on 1 November 2021, is the first omnibus law in China that regulates PI, in particular the processing of PI of individuals within China as well as some processing activities performed outside China. The PIPL imposes obligations on data controllers (although the actual terminology for data controllers in the PIPL is the slightly confusing: 'personal information processor').

Under the Civil Code of the PRC, which took effect on 1 January 2021, individuals have express and codified rights to the privacy and protection of PI.

The PIPL, the DSL and the CSL are to be accompanied by an extensive series of implementing regulations in the form of guidelines and measures. Some of these implementing regulations have already been finalised (eg, the Revised Cybersecurity Review Measures, effective 15 February 2022, and the Internet Information Service Algorithmic Recommendation Management Provisions, effective 1 March 2022), but many are yet to be formulated.

A number of these regulations are presently in draft form and, while non-binding in such form, compliance is advisable as they reflect regulatory attitudes.

Some relevant draft regulations, both general and industry-specific, include the:

- Measures on Security Assessment of the Cross-Border Transfer of Personal Information (issued 13 June 2019);
- Measures on Data Security Management (issued 28 May 2019);
- Notice on Strengthening Cybersecurity Work in the Internet of Vehicles (Smart Connected Vehicles) (issued 22 June 2021);
- Measures on Data Export Security Assessment (issued 29 October 2021);
- Regulations on Network Data Security Management (issued 14 November 2021);
- Mobile Internet Application Programme Information Service Management Regulations (issued 5 January 2022);
- Guidelines for the Identification of Important Data (issued 13 January 2022);
- Internet Information Service Deep Synthesis Management Provisions (issued 28 January 2022);
- Measures on Industry and Information Technology Data Security Management (issued 10 February 2021);
- Regulations on the Administration Of Internet Pop-Up Push Notifications (issued 2 March 2022); and
- Regulations on the Online Protection of Minors (issued 14 March 2022).

Any references to China refer to mainland China and do not include Macau and Hong Kong, which are subject to separate laws and regulations.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

There is no single authority that is responsible for overseeing the enforcement of data protection laws in China, but the main authority is the Cyberspace Administration of the PRC (CAC) and its respective local offices. Multiple regulatory authorities are granted various investigatory and enforcement powers concerning data protection matters, including the ability to impose administrative sanctions. Under the PIPL, the departments that perform PI protection duties are responsible for enforcing the PIPL. However, people's procuratorates (eg, the equivalent to a public prosecutor in China), statutorily designated consumer organisations and organisations designated by the CAC may also file a lawsuit with a people's court against data controllers that violate the PIPL.

The CAC is the primary data protection regulator under the CSL, DSL and PIPL and has broad responsibilities and enforcement powers. The Cybersecurity Review Office, which is based in the CAC, is responsible for formulating cybersecurity review systems and standards and organising cybersecurity reviews.

The Ministry of Industry and Information Technology and the telecommunication administrations at the provincial level are tasked with overseeing the protection of PI in the telecoms and information services sector, including the supervision and administration of PI of telecommunication and internet users.

The Ministry of Public Security (MPS) is China's key police and security authority and is granted wide investigatory and enforcement powers to combat cybercrimes. The MPS is empowered to carry out inspections and criminal investigations, which may include inspecting the servers and systems of CII operators and network operators.

The State Administration for Industry and Commerce and its local counterparts are responsible for the supervision and administration of PI of consumers, under the Provisions on Regulating the Market Order of Internet Information Services.

Industry-specific regulations may also be enforced by the relevant industry regulators.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There is no legal obligation on the Chinese authorities to cooperate with data protection authorities in other jurisdictions.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Any violations of the laws relating to data protection may result in fines, corrective orders or warnings, public naming and shaming, confiscation of illegal gains, orders for the suspension or shutting down of operations, the shutting down of websites, revocation of business permits or licences or potential criminal liability.

Judicial review of data protection authority orders

5 Can PI owners appeal to the courts against orders of the data protection authority?

There are no specific mechanisms that allow data controllers to appeal against orders of the relevant data protection authority. However, as enforcement orders are administrative acts, the data controller may nonetheless challenge the enforcement orders by applying for an administrative reconsideration or filing an administrative lawsuit through China's courts.

SCOPE

Exempt sectors and institutions

6 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The obligations under the Cybersecurity Law (CSL) apply to critical information infrastructure (CII) providers and network operators. CIIs include key sectors such as finance, transportation, energy, water, government and communications, and any other industries where the destruction, loss of function or data leakage by such industry could result in serious damage to national security, national economy and people's livelihood and public interests. Network operators are broadly defined under the CSL as owners or managers of networks and providers of network services, and could potentially apply to any entity that uses IT systems in China or operates a Chinese website, irrespective of their industry.

The Data Security Law (DSL) applies to handling processing activities inside China and, in certain circumstances, outside China. Given the expansive definitions of 'data' and 'data processing', the DSL applies not only to internet service providers and big tech companies, but all sectors and types of organisations involved in the recording and processing of information.

Similarly, the Personal Information Protection Law (PIPL) applies to PI processing within China and, in some circumstances, on processing activities outside China. Given the broad definitions of 'PI' and 'PI processing', it is clear that the PIPL applies to both the public and the private sectors.

Interception of communications and surveillance laws

7 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Yes. The PIPL addresses electronic marketing insofar as it establishes rules on the use of automated decision-making. The PIPL also grants the state a wide array of powers when investigating PI processing activities, including:

- interviewing parties and investigating circumstances related to PI processing activities;
- consulting and reproducing a party's contracts, records and receipts, as well as other relevant material related to PI processing activities;
- conducting on-site inspections and investigations of suspected unlawful PI processing activities; and
- inspecting equipment and articles relevant to personal PI processing activities, and when there is evidence the equipment or articles are used to engage in illegal PI processing activities, after receiving approval from the head of the relevant department, they may seal or confiscate them.

These may allow the state to access private and individual communications when investigating PI processing activities.

Regarding the interception of communications, article 40 of the PRC Constitution Law further grants the state power to obtain access to private and individual communications in situations related to public security or criminal investigations. Article 13 of the PRC Counter-espionage Law also provides that national security authorities are entitled to inspect 'electronic communication instruments, appliances, other similar equipment belonging to any organisation or individual' for purposes of countering espionage activities. Further, article 65 of the Telecommunications Regulations grants relevant security authorities the power to carry out examinations of private telecommunications based on national security or criminal investigations.

Regarding electronic marketing, the Measures for the Administration of Internet Email Services 2006 requires, among other things, that express consent of data subjects has been obtained before sending any email advertisements to recipients via an opt-in approach, and that the word 'ad' or 'advertisement' in the subject line of the email advertisement in English or Chinese be included to denote the commercial nature of the email.

Other laws

8 Are there any further laws or regulations that provide specific data protection rules for related areas?

- Employee information: the Labour Contract Law governs the collection and use of employee's personal information for the purposes of recruitment and employment.
- Internet service providers: the Regulations on Standardising the Order of the Internet Information Service Market 2011 requires that data subjects are clearly informed by internet service providers of the collection method and purpose for collecting and processing their personal information. In 2022, the CAC passed several

regulations and issued draft regulations to further regulate the collecting and processing of personal information in the context of specific internet service provider activities, such as push notification, algorithmic recommendation and deep synthesis (deep fake) service providers. These regulations (draft or otherwise) were issued pursuant to a number of laws, including the CSL and the PIPL.

- Credit information: credit reporting agencies and other companies that collect credit information are subject to the data localisation requirement under the Administrative Regulations on the Credit Reporting Industry 2013.
- Personal finance information: all banks in China are required by the People's Bank of China to store, use and process all personal information within China.
- Children: on 1 October 2019, the new Online Protection of Children's Personal Data Regulation came into force, which sets out requirements aimed at protecting children's personally identifiable information. It is in line with the CSL. On 14 March 2022, the CAC released new draft regulations on the online protection of minors pursuant to the Law on Protection of Minors, the CSL and the PIPL and to impose more value-based obligations on the online product and service providers, data controllers and manufactures or sellers of smart terminals.
- Other various laws, regulations and guidelines that also address the protection of personal information include:
  - the Decision on Strengthening Protection of Network Information;
  - the Law on the Protection of Consumer Rights and Interests;
  - the Measures for the Administration of Online Transactions;
  - the Provisions on Protecting the Personal Information of Telecommunications and Internet Users;
  - Several Provisions on Regulating the Market Order of Internet Information;
  - the Medical Records Administration Measures of Medical Institutions;
  - the Measures for Administration of Population Health Information;
  - the Measures for the Administration of Internet Email Services;
  - the Standards for the Assessment of Internet Enterprises' Protection of Personal Information, which are not binding; and
  - the Administrative Provisions on Short Message Services.

PI formats

9 | What categories and types of PI are covered by the law?

All types of PI are covered by the CSL, the DSL, the PIPL and other related regulations.

'Personal information' in the PIPL refers to various information related to identified or identifiable natural persons recorded electronically or by other means, but does not include anonymised information.

Under the CSL, 'personal information' is defined as all kinds of information recorded in electronic or other forms that can be used independently or in combination with other information to identify a natural person's personal identity, including, but not limited to, their names, dates of birth, identity numbers, biological data, addresses and telephone numbers. This definition is also in line with the definition of 'personal information' under the new Civil Code of the PRC, which also includes email addresses, health information and location information.

The DSL applies not only to PI but to all kinds of data; 'data' is defined as any record of information, whether in electronic or non-electronic form.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The law has extraterritorial effect.

The PIPL applies both to the processing of personal information of individuals within China and to any processing activities performed outside China, if this processing:

- is for the purpose of providing products or services to individuals located in China;
- is for the purpose of analysing or evaluating the activities of individuals located in China; or
- falls within any other circumstances specified under local laws or regulations.

Likewise, the DSL also has extraterritorial effect and applies to data processing activities conducted outside China that may harm or damage national security, the public interest or the lawful rights and interests of Chinese citizens or organisations.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Yes. Between the DSL, which applies to all data (not just PI) processing activities, and the PIPL, which applies to all PI processing activities, all processing or use of PI is covered.

The PIPL distinguishes between data controllers and data processors, and imposes obligations on data controllers, who remain responsible for the actions of the data processors they engage.

Data processors are only statutorily obliged to adopt necessary measures to protect the PI entrusted to them in accordance with the PIPL and other relevant laws and regulations, and to assist the data controller in complying with their obligations under the PIPL.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes. While notification and consent have been the only legal basis for processing PI under the Cybersecurity Law, the Personal Information Protection Law (PIPL) provides for the following additional grounds:

- where necessary for the conclusion or performance of a contract or carry out human resources management;
- where necessary for the performance of statutory responsibilities or statutory obligations;
- where necessary to respond to a public health emergency or to protect a data subject's interest or safety in an emergency;
- where necessary to carry out activities in the public interest;
- where the relevant PI, which has either been disclosed by the relevant data subject or otherwise been legally disclosed, is processed within a reasonable scope according to law; and
- other circumstances as provided by laws or regulations.

The PIPL also sets out detailed provisions for notification and consent. In particular, it requires data controllers to obtain separate consent from data subjects where: sensitive PI is processed; the PI is provided

by the data controller to another data controller; the PI processed is publicly disclosed; or the PI is transferred outside of China.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Yes. Under the PIPL, more stringent rules are imposed on sensitive PI. Sensitive PI refers to PI that, once leaked or illegally used, may easily cause harm to the dignity of natural persons or cause grave harm to personal or property security. This includes biometric information, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking and the personal information of minors under the age of 14.

In addition, the Personal Information Security Specification 2020 (the 2020 PI Specification) imposes additional requirements on personal biometric information, which includes personal genes, fingerprints, voiceprints, palm prints, auricles, irises and facial recognition data.

Under the Regulation on Cyber Protection of Children's Personal Information, additional requirements are also imposed on network operators collecting, using or disclosing the personal information of children under the age of 14.

In particular, network operators are required to provide a privacy policy and terms of use that are specifically tailored to, and appoint specific personnel to be in charge of, the protection of children's personal information. Network operators must also comply with certain requirements when obtaining consent from a child's guardian for the collection, use or disclosure of the child's personal information. For example, network operators must notify the child's guardian of the purposes for which the child's personal information will be collected or used prominently and clearly before obtaining their consent. Fresh consent must also be obtained from the guardian where the use of the child's personal information goes beyond the initially notified purposes. Additional security requirements will also apply concerning the handling of children's personal information.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Yes. The Personal Information Protection Law (PIPL) requires data controllers, prior to collecting and processing PI, to provide to the data subject certain information that has to be displayed or presented in a conspicuous manner and in clear and understandable language. This information includes:

- the name and contact details of the data controller;
- the purpose and the method of PI processing activities;
- the categories of processing PI;
- the retention period;
- the methods for data subjects to exercise their rights provided under the PIPL; and
- other items that laws or administrative regulations stipulate as having to be notified.

Data controllers must also notify data subjects when there is a change in any of the above information.

Exemptions from transparency obligations

15 | When is notice not required?

Notice is not required:

1 if any laws or administrative regulations provide that confidentiality must be preserved or notification is not necessary; or
2 in an emergency, where it is not possible to notify data subjects in a timely manner to protect the life, health or property of a data subject.

In the case of (2), the data controller must provide notice to the data subject after the emergency situation has subsided.

Irreversibly anonymised PI is not subject to the PIPL.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes. The PIPL states that processing of PI should be carried out in such a way so to ensure the quality, accuracy and completeness of PI to avoid adverse effects on the data subjects' rights and interests.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Yes. The PIPL states that processing of PI should be carried out in such a way so to ensure the quality, accuracy and completeness of PI to avoid adverse effects on the data subjects' rights and interests.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Yes. The PI must only be retained for as long as necessary to realise the processing purposes.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes. PI can only be used for for the purposes initially notified to the data subject.

If the data controller wishes to use the PI for a purpose that is different from the purposes initially notified to the data subject, or where there is a change to the means of processing or categories of PI being collected and used, the data controller is required to obtain fresh consent from the data subject.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Yes. Under the PIPL, data controllers who intend to use PI for automated decision-making must ensure that such processing is carried out in a manner that is transparent, fair and just. The PIPL also prohibits treating data subjects in an unreasonably differentiated manner (eg, differentiated trade prices).

Data controllers are also expected to provide data subjects with a convenient method to refuse consent or be given an option to

opt out where push notifications are sent on the basis of automated decision-making.

Where the use of automated decision-making has a major impact on the rights and interests of the data subjects, the data subject has additional rights to require data controllers to provide an explanation of the circumstances or refuse to be subject to decisions made solely on the basis of automated decision-making.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Data controllers are required to implement all necessary measures to ensure the security of the PI they process, which includes the following measures to prevent any unauthorised access, leakage, modification or loss of PI:

- formulate internal management structures and operating rules;
- implement categorised management of personal information;
- adopt corresponding technical security measures such as encryption and de-identification;
- set reasonable operational limits for PI handling, and regularly conduct security education and training for employees;
- devise and implement PI incident response plans; and
- other measures provided in laws or administrative regulations.

Under the Information Security Technology – Personal Information Security Specification 2020 (the 2020 PI Specification), PI owners are required to adopt security measures, such as encryption, when transmitting and storing personal sensitive information. PI owners are advised to follow the relevant national standards for password management when employing cryptographic techniques.

The 2020 PI Specification also requires all personal biometric information to be stored separately from other personal information. PI owners should also not store any 'original' biometric information (eg, samples and images, etc) and instead employ measures such as retaining only abstract information and deleting raw data after use.

Under the Regulation on Cyber Protection of Children's Personal Information, where a network operator collects any personal information of children under the age of 14 and subsequently outsources the handling of or otherwise transfers such personal information to third parties, the network operator should conduct a security assessment on the relevant third party and ensure that the parties agree on the scope of the third party's authority concerning the handling of such information.

Article 1038 of the Civil Code of the PRC also imposes a general obligation on PI owners to ensure the safety of the personal information that they have collected and stored through technical or other necessary measures, which includes prevention of data breaches, tampering or data loss.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Yes; when a leak, destruction, distortion or loss of PI occurs, or might have occurred, data controllers must promptly inform data subjects and report this to the authorities unless data controllers adopt measures that are able to effectively avoid any harm created by the PI leak, destruction, distortion or loss, in which case the data controllers are permitted not to notify data subjects. However, this decision not to notify data subjects can be overridden by the relevant authority, who can still decide that notification to the data subjects is required.

Further, where the data breach results in harm to individuals or organisations, data controllers must notify the affected parties within three working days. When a leak, destruction, loss or other such data security incident involves the personal information of 100,000 individuals or more, data controllers are required to provide the city-level cyberspace administration and the relevant regulatory authorities with: a basic report of the incident within 8 hours of the incident; and a full investigation and assessment report within 5 working days after the conclusion of the incident response.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Yes. Under the Personal Information Protection Law (PIPL), data controllers have an obligation to formulate internal management structures and operating rules to ensure that their personal information processing conforms to the provisions of laws and administrative regulations, and prevents unauthorised access as well as PI leaks, distortion or loss.

The PIPL also requires data controllers to audit their PI processing and compliance with the laws and administrative regulations on a regular basis.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

No. Under the PIPL, only data controllers that process PI of a volume above a certain threshold (to be specified by the Cyberspace Administration (CAC)) are required to appoint a data protection officer (DPO). This threshold has yet to be specified by the CAC.

However, some guidance on this threshold may be gleaned from the non-binding Information Security Technology – Personal Information Security Specification 2020 (the 2020 PI Specification), which requires organisations that fall into one or more of the following categories to appoint a DPO:

- the main business involves the processing of personal information and the organisation employs over 200 employees;
- the organisation processes the personal information of more than 1 million people or expects to process the personal information of more than 1 million people within the coming 12 months; or
- the organisation processes the sensitive personal information of more than 100,000 people.

The DPO will be responsible for supervising the data processing activities of the data controller and ensuring that the protection measures are being implemented. The data controller must also report to the relevant local data protection authority the name and contact details of the appointed DPO.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Yes; data controllers must keep PI impact assessment reports and processing records for at least three years.

The Draft Online Security Management Regulations introduce other potential obligations for data controllers:

- when providing important data to third parties, to retain data subject consent records and daily records on the provision of PI, and examination and approval records and daily records on sharing, trading or entrusting the processing of important data, for a period of at least five years; and
- when providing data abroad, to retain related daily records and outbound data transfer examination and approval records for a period of three years or more.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Yes. Data controllers are required to conduct a PI impact assessment prior to:

- processing sensitive PI;
- using PI in automated decision-making;
- entering into a data processing arrangement, transferring PI to another data controller or disclosing PI;
- transferring PI outside China; and
- other PI processing activities with a major influence on data subjects.

The risk assessment should consider:

- whether the purposes for, and processing methods of, the PI are lawful, legitimate and necessary;
- the influence on a data subject's rights and interests;
- possible security risks; and
- whether protective measures undertaken are legal, effective and appropriate when balanced against the degree of risk.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

There are no specific or explicit obligations in relation to how PI processing systems must be designed. However, given the high thresholds necessary to process certain types of information (eg, requiring separate consent prior to processing sensitive PI or transferring PI outside of China), as well as the data localisation requirements, data controllers may require privacy-by-design mechanisms to ensure compliance with the PIPL.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no general requirement for data controllers to register with the supervisory authority. However:

- data controllers that process PI over a certain threshold are required to appoint a date protection officer, whose details (eg, name and contract method) must be notified to the relevant supervisory authority; and
- data controllers outside China that process the PI of natural persons in China are required to appoint a representative in China to be responsible for matters PI they process and report the representative's name and contact method to the relevant supervisory authority.

Other transparency duties

29 | Are there any other public transparency duties?

Other transparency duties include requirements for data controllers to:

- notify data subjects of the recipient's identity and contact methods in cases where it is necessary to transfer PI for the purposes of mergers, separations, dissolutions, declaration of bankruptcy and other similar reasons; and
- obtain the separate consent of the data subject when they transfer PI to another data controller and notify the data subject of the recipient's identity, contact methods, processing purposes and methods, and categories of PI.

Under the PIPL, data controllers are also required to obtain separate consent from data subjects when:

- processing sensitive PI;
- transferring PI out China;
- transferring PI to other data controllers;
- disclosing PI; and
- using images and other distinguishing identity or biometric characteristic information collected via image collection (eg, CCTV cameras) or personal identity recognition equipment (eg, facial recognition devices) in public areas for any purpose other than to safeguard public security.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Under the Personal Information Protection Law (PIPL), data controllers are required to enter into a data processing agreement (DPA) with its data processors. The DPA must include provisions addressing the:

- time limit for storing PI;
- processing methods;
- categories of PI to be processed;
- security measures;
- rights and duties of both parties;
- rights of the data controller to exercise oversight over the data processing activities of the data processor;
- return of PI if the DPA is void, does not take effect or has been terminated; and
- restrictions on sub-processing without the data controller's prior consent.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Any disclosure of PI or transferring of PI to another data controller must be subject to the data subject's separate consent.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Yes. Under the PIPL, prior to transferring PI out China, data controllers are required to:

- notify data subjects of:
  - the foreign recipient's identity and contact methods;
  - processing purposes and methods;
  - categories of PI; and
  - methods for data subjects to exercise their rights under the PIPL with the foreign recipient; and
- obtain the data subject's separate consent prior to such transfer.

Data controllers are also required to implement necessary measures to ensure that foreign recipients provide the PI with an equivalent standard of protection as provided under the PIPL.

Furthermore, data controllers transferring PI out of China must also meet one of the following conditions:

1 passing a security assessment organised by the Cyberspace Administration (CAC);
2 undergoing PI protection certification conducted by a specialised body designated by the CAC;
3 entering into standard form contract issued by the CAC with the foreign recipient; or
4 other conditions provided in laws or regulations or by the CAC (eg, any international agreements between China and foreign recipient countries allowing PI to be transferred).

However, the CAC has yet to:

- designate a specialise body to conduct the PI protection certificate mentioned in (2); although, the National information Security Standardisation Technical Committee issued the draft Technical Specifications for Certification of Cross-border Handling of PI in April 2022; or
- issue the standard form contract mentioned in (3); although, some pertinent provisions have been specified in the draft Outbound Data Transfer Measures and the draft Online Data Security Management Regulations.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The draft Online Data Security Management Regulations stipulate that the conditions for further transfer (after transferring PI out of China) must be agreed with the data subject in advance. Read with the other obligations under the PIPL, this means that the onus is on the data controller to ensure that further transfers of PI are not carried out without its consent as it would need, or have needed, to obtain the data subject's consent.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No. However, data stored within China may not be provided to foreign judicial and law enforcement bodies without the prior approval of the relevant authorities.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, except where laws or administrative regulations provide that confidentiality must be preserved or where doing so would impede the regulatory bodies' abilities to fulfil their statutory duties and responsibilities.

When data subjects exercise their rights to access their PI, data controllers are required to provide it in a timely manner.

Other rights

36 | Do individuals have other substantive rights?

Yes. Data subjects also have the rights to:

- data portability (subject to certain conditions to be designated by the Cyberspace Administration of the PRC (CAC);
- correction (data controllers are to verify PI and correct or complete it in a timely manner);
- deletion in the following circumstances;
  - the processing purposes have been completed or are impossible to complete, or the PI is no longer necessary to achieve the processing purpose;
  - data controllers cease the provision of products or services, or the retention period has expired;
  - the data subject withdraws their consent;
  - data controllers process PI in violation of laws, administrative regulations or agreements; or
  - other circumstances provided by laws or administrative regulations;
- opt out of the use of their PI in automated decision-making for the purposes of push notifications and commercial activities;
- where the use of automated decision-making has a major impact on the data subject's rights and interests, request that data controllers explain the circumstances, and may refuse to allow data controllers to make decisions solely on the basis of automated decision-making;
- request an explanation of the data controller's PI processing rules (eg, their privacy policy);
- where a deceased person has not made alternative arrangement prior to their death, exercise the rights of a deceased person may as their next of kin; and
- an explanation where their requests to exercise their data subject rights are rejected by the data controller.

Where the retention period provided by law or relevant regulations has not expired, or deleting the PI is technically difficult to achieve, data controllers are required to cease processing the PI except for storing and taking adequate security measures.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under the Personal Information Protection Law (PIPL), data controllers are liable to compensate data subjects when their processing infringes upon PI rights and interests and results in harm to the data subject, and data controllers are unable to demonstrate that they had taken all reasonable steps to avoid such infringement.

It is unclear whether injury to feelings is sufficient, but there is a potential that it may be. Under article 69 of the PIPL, the compensation is to be determined on the basis of the loss to the data subject or the data controller's consequent gains. However, where the loss to the data subject or gain to the data controller is difficult to ascertain, compensation is to be determined on the basis of 'practical conditions'. We expect further clarification on this to be issued in the future.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Where data controllers violate provisions of the PIPL, people's procuratorates (the equivalent of a public prosecutor in China), statutorily designated consumer organisations and organisations designated by CAC may file a lawsuit with a people's court against the data controller. Penalties arising from a violation of the PIPL (eg, fines of up to 50 million yuan or 5 per cent of annual revenue, and suspension of business activities) may also be enforced directly by the regional CAC office.

Where data controllers reject a data subject's request to exercise their rights under the PIPL, the data subject may file a lawsuit with a people's court against the data controller.

Further, given that data privacy rights have been codified in the Civil Code, individuals also have the right to take civil action against those who breach these rights.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

The Personal Information Protection Law (PIPL) provides exceptions to the requirement to obtain express consent from data subjects, including but not limited to:

- where necessary to conclude or fulfil a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labour rules and structures and lawfully concluded collective contracts;
- where necessary to fulfil statutory duties and responsibilities or statutory obligations;
- where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;
- processing personal information within a reasonable scope to implement news reporting, public opinion supervision and other such activities for the public interest; and
- when processing personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of the PIPL.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

To the extent that cookies amount to personal information (which is defined as information that can be used alone or in combination with other information to identify an individual), they will be governed by the Cybersecurity Law (CSL), the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) and related regulations and measures. Otherwise, no legislation specifically governs the use of cookies.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Under the Decision on Strengthening Protection of Network Information and the law on the Protection of Consumer Rights and Interests, commercial information cannot be sent to consumers:

- unless the consumer has requested the information;
- unless the consumer has consented to receive the information; or
- if the consumer has expressly refused to receive the information.

Under the Measures for the Administration of Internet Email Services, where an email recipient has clearly consented to receive emails containing commercial advertisements, but later withdraws this consent, the sender must stop sending such emails unless otherwise agreed by both parties. When sending emails containing commercial advertisements, the sender must provide its contact information, including its email address, and a guarantee that this contact information will remain valid for 30 days.

Under the Administrative Provisions on Short Message Services, short message service providers and short message content providers must not send commercial messages to users without their consent or request, and must explain the type and frequency of the commercial messages that will be sent. A user's failure to respond will be regarded as a refusal of consent.

The Cyberspace Administration (CAC) also issued draft regulations on the administration of internet pop-up push notifications, which apply to all owners and operators of operating systems, terminal devices, application software, websites and other such services that provide push notification services in China.

Targeted advertising

42 | Are there any rules on targeted online advertising?

Yes. The Internet Information Service Algorithmic Recommendation Management Provisions (the Algorithm Provisions) issued pursuant to the CSL, PIPL and DSL address algorithm recommendation technologies such as product recommendations, personalised advertisements and filtering.

Other than providing high-level regulatory principles for algorithm operators, the Algorithm Provisions impose requirements on algorithm operators, which include:

- complaint mechanisms for users and the public to seek redress;
- regular assessments of their algorithms to ensure that the algorithmic models 'do not violate laws and regulations or ethics and morals' such as addiction or excessive consumption;
- prohibiting the use of algorithms on social networking sites to over-recommend or manipulate search results or topic lists, exercise control over popular search terms and other arrangements of information or to carry out acts that may influence public opinion; and
- providing consumers with the right to turn off algorithmic recommendation services or request the service provider to provide services not targeting their personal characteristics. Consumers also have the right to request the service provider delete user tags targeting their personal characteristics for algorithm recommendation services.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Yes. Sensitive personal information refers to PI that, once leaked or illegally used, may easily cause harm to the dignity of natural persons or cause grave harm to personal or property security. This includes biometric information, religious beliefs, specially designated status, medical health, financial accounts and individual location tracking, as well as the personal information of minors under the age of 14.

Under the PIPL, prior to processing any sensitive personal information, data controllers must conduct an internal PI impact assessment, taking into account:

- whether or not the PI handling purposes and handling methods, etc, are lawful, legitimate and necessary;
- the influence on data subject's rights and interests, and the security risks; and
- whether protective measures undertaken are legal, effective and suitable to the degree of risk.

Further, data controllers that process any sensitive personal information must obtain separate consent from data subjects. In addition to the standard PIPL notification requirements, data controllers must also notify data subjects of the:

- necessity and influence on the individual's rights; and
- data controller's interests in handling the sensitive PI.

Where data controllers process the PI of minors under the age of 14, they are required to obtain the consent of the parent or other guardian of the minor and to formulate specialised PI processing rules.

To process sensitive PI, the PIPL also contemplates that there may be other laws or administrative regulations that require:

- written consent; or
- a relevant administrative licence.

Profiling

44 | Are there any rules regarding individual profiling?

Yes. Automated decision-making is defined in the PIPL as the activity of using computer programs to automatically analyse or assess personal behaviours, habits, interests or hobbies, or financial, health, credit or other status, and make decisions based on the information assessed.

Prior to using PI to conduct automated processing, data controllers must conduct an internal PI impact assessment, taking into account:

- whether or not the PI handling purposes and handling methods, etc, are lawful, legitimate and necessary;
- the influence on data subject's rights and interests, and the security risks; and
- whether protective measures undertaken are legal, effective and suitable to the degree of risk.

Data controllers are also required to conduct automated processing in a manner that is transparent, fair and just, and may not treat data subjects in an unreasonably differentiated manner (eg, differentiated trade prices).

Data controllers are also expected to provide data subjects with a convenient method to refuse or given an option to opt out where push notifications are sent on the basis of automated decision-making.

Where the use of automated decision-making has a major impact on the rights and interests of the data subjects, the data subject has additional rights to require data controllers to provide an explanation of the circumstances or refuse to be subject to a decision made solely on the basis of automated decision-making.

MAYER | BROWN

Gabriela Kennedy
gabriela.kennedy@mayerbrown.com

Joshua T K Woo
joshua.woo@mayerbrown.com

16th–19th Floors
Prince's Building
10 Chater Road
Central
Hong Kong
Tel: +852 2843 2211
www.mayerbrown.com

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

In July 2019, the Ministry of Industry and Information Technology issued the Measures on Security Assessments for Cloud Computing Services to regulate cloud computing providers that offer cloud computing services to the Chinese government.

Cloud computing is also one of the specific types of critical information infrastructure (CII) sectors listed in the CSL, which means that organisations that offer cloud computing services must comply with the more stringent obligations imposed on CII operators under the CSL.

Further, the Information Security Technology – Baseline for Classified Protection of Cybersecurity issued in May 2019 also stipulates additional security requirements concerning the use of cloud computing.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Given that the Personal Information Protection Law (PIPL) and Data Security Law are relatively new laws, many of the implementing regulations are still in draft form and subject to further amendments. Notably, when looking at published enforcement decisions, a majority of the PI-related decisions are still being issued on the basis of the Cybersecurity Law and not the PIPL.

There have been more rules targeting specific industry sectors issued in the past year (eg, automobiles and the online protection of minors), which reflect the Chinese government's recognition of the varied forms of PI in this day and age.

While a majority of the recent regulations are still in draft form, the Chinese government's latest efforts to rein in big tech companies operating in China is evident from its somewhat expedited passing of the Revised Cybersecurity Review Measures and Internet Information Service Algorithmic Recommendation Management Provisions in February and March 2022. Similarly, given the popularity of mobile applications (and their relation with big tech in China), there has also been increased

scrutiny on the data collection and use practices of smartphone applications. This has led to the Cyberspace Administration's issuance of various draft regulations in the first quarter of 2022, such as the:

- Mobile Internet Application Program Information Service Management Regulations;
- Internet Information Service Deep Synthesis (Deepfake) Management;
- Regulations on the Administration of Internet Pop-up Push Notifications;
- Internet Information Service Algorithmic Recommendation Management Provisions; and
- Regulations on the Online Protection of Minors (issued 14 March 2022).

These regulations are aligned with existing Chinese data protection laws and are in keeping with the government's broader efforts to reduce the influence of big tech.

Lastly, new e-commerce rules have recently been announced in a bid to regulate the boom in e-commerce platforms and surge in popularity of live stream e-commerce sales, particularly in the wake of the pandemic. The Online Live Marketing Management Measures (for Trial Implementation) took effect on 25 May 2021 and, in particular, article 6 of the new rules require the establishment of mechanisms and measures for the protection of personal data. These new rules will work alongside the E-Commerce Law 2019 in the regulation of e-commerce activities.

Moreover, to accommodate the growth of the innovation economy, some new regulations focusing on data management and data processing activities in new emerging industry sectors have been introduced (eg, the Several Provisions on the Management of Automobile Data Security (for Trial Implementation) that came into force on 1 October 2021).

France

Benjamin May and Marianne Long
Aramis Law Firm

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The legislative framework for the protection of PI in France is one of the oldest in Europe, being based on the Law on Computer Technology and Freedom of 6 January 1978 (LIL). This law has been amended several times, and especially by:

- Law No. 2004-801 of 6 August 2004 to implement the provisions of Directive 95/46/EC;
- Law No. 2016-1321 of 7 October 2016, which anticipates the implementation of certain provisions of Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR);
- Law No. 2018-493 of 20 June 2018, which implements the GDPR in France and further amend the LIL; and
- Ordinance No. 2018-1125 of 12 December 2018 and Decree No. 2019-536 of 29 May 2019, which complete at the legislative level the compliance of the national law with the GDPR and redraft the LIL for better readability and understanding of the law.

As a regulation, the GDPR has been in effect in France since 25 May 2018.

Further, the following international instruments on privacy and data protection also apply in France:

- Council of Europe Convention 108 on the protection of privacy and trans-border flows of personal data;
- the European Convention on Human Rights and Fundamental Freedoms (article 8 on the right of respect for private and family life); and
- the Charter of Fundamental Rights of the European Union (article 7 on the right to respect for private and family life and article 8 on the right to the protection of personal data); and
- European Data Protection Board guidelines; and
- Directive 2002/58/EC on privacy and electronic communications (for cookies).

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The data protection authority in France is the National Commission for Data Protection and Liberties (CNIL). The CNIL is an independent public body entrusted with the following powers.

Control and investigation powers

The CNIL is vested with investigation and control powers that allow its staff to have access to all professional premises and to request, on the spot, all necessary documents and to take a copy of any useful information. CNIL staff can also access any computer programs linked to the processing of PI and recorded information. The CNIL can also conduct a documentary control where a letter accompanied by a questionnaire is sent to a PI controller and processor to assess the conformity of processing operations carried out by them or an online investigation, in particular by consulting data that are freely accessible or made directly accessible online, including under a fake identity.

Each of these controls can be used in a complementary manner.

A statement is drawn up at the end of the inspection, listing all the information gathered by the inspectors and the observations they have made.

The audited company may not invoke professional secrecy to justify any refusal to allow CNIL auditors access to computer programs or to communicate documents to them, unless the data is related to correspondence between a lawyer and his or her client, or is covered by the secrecy of journalistic processing.

In 2020, it carried out 6,500 investigative acts, including 247 formal control procedures.

In 2021, the CNIL focuses its inspection activities on three priority areas: website cybersecurity, health data security and the use of cookies.

According to the CNIL, these three themes will represent around 20 per cent of the formal control procedures that will be carried out in 2021. As in previous years, controls will also be initiated following:

- complaints and claims addressed to the CNIL;
- topical issues requiring the control of the processing implemented; and
- corrective measures (formal notices and sanctions, etc) requiring new checks.

Powers of sanction

The maximum threshold of penalties that the CNIL can pronounce has been increased from €150,000 to €20 million or 4 per cent of world turnover for companies since GDPR enactment.

The CNIL can now compel sanctioned entities to inform each data subject individually of this sanction at their own expense.

The fine of €50 million pronounced by the CNIL against Google for not properly informing its users on how data is collected across its services to present personalised advertisements is a prime example of the strengthening of its financial sanctioning power.

In 2019, decisions rendered by the CNIL showed it can deviate from its classic approach and impose financial penalties against defaulting companies without prior formal notification.

Indeed, on 25 July 2019, the CNIL imposed a fine of €180,000 on Actives Assurances, an insurance intermediary specialising in the

online distribution of automobile insurance contracts, for having insufficiently protected the data of the users of its website.

Within the framework of this power of sanction, the entry into force of the GDPR has increased the CNIL's range of sanctions. Three decisions taken at the end of 2020 are quite significant on this subject and are based on non-compliance with both the GDPR and the provisions of the LIL, particularly on the issue of cookies.

After receiving several complaints, the CNIL imposed financial penalties against two companies of the Carrefour group for GDPR infringements concerning the information given to individuals and in particular, with respect of their rights, by imposing a penalty of €2,250,000 against Carrefour France and €800,000 against Carrefour Banque. However, the CNIL did not issue an injunction to comply since it noted that significant efforts had already been made to address the infringements.

On 7 December 2020, the CNIL's restricted panel fined Google LLC and Google Ireland Limited a total of €100 million for having placed advertising cookies on the computers of users of the search engine google.fr without prior consent or satisfactory information.

On 10 December 2020, the CNIL also fined Amazon Europe Core a total of €35 million for having deposited advertising cookies with no prior consent and satisfactory information (article 82 of the LIL).

In this case, a client of Active Assurances discovered that he could easily access the personal data of other clients from his account. He alerted the CNIL, which carried out an online check. That same day, the CNIL alerted Active Assurance of this data breach and requested the company address it, without this request being a prior formal notification. A few days later, when the company informed the CNIL that measures had been taken, a new onsite inspection revealed that the measures were not sufficient to secure the personal data in question and the CNIL considered that Active Assurance had failed to comply with its obligation of security under article 32 of the GDPR and pronounced a fine of €180,000.

This is not an isolated case. On 28 May 2019, the CNIL issued a fine of €400,000 against Sergic, a real estate company, for data security breaches and non-compliance with the data retention period under the GDPR.

The CNIL must respond to numerous complaints (more than 14,000 in 2021) despite the constant increase in the number of corrective measures it issues (18 sanctions and 135 formal notices were issued in 2021). On 24 January 2022 and then on 8 April 2022, the CNIL's repressive procedures were modified: a simplified procedure was notably created for less complex cases. This reform will enable the CNIL to act more effectively in the face of the increasing number of complaints since the GDPR came into force.

Regulatory powers

CNIL powers have recently been extended; it will have to be consulted for every bill or decree related to data protection and processing. Opinions will automatically be published.

The CNIL is also entrusted with the power to certify, approve and publish standards or general methodologies to certify the compliance of personal data anonymisation processes with the GDPR, notably for the re-use of public information available online.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

If the owner or processor of PI carries out cross-border processing either through multiple establishments in the European Union or with only a single establishment, the supervisory authority for the main or single establishment acts as the lead authority in respect of that cross-border processing.

As the lead authority, the CNIL must cooperate with the data protection authorities in other EU member states where the owner or the processor is established, or where data subjects are substantially affected, or authorities to whom a complaint has been made. Specifically, the CNIL must provide information to other data protection authorities and can seek mutual assistance from them and conduct joint investigations with them on their territory.

More generally, the CNIL is required to assist other data protection authorities in the form of information or carrying out 'prior authorisations and consultations, inspections and investigations'. The European Commission can specify forms and procedures for mutual assistance. The CNIL could also participate in joint investigation and enforcement operations with other data protection authorities, particularly when a controller has an establishment on its territory or a significant number of its data subjects are likely to be substantially affected.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Failure to comply with data protection laws can result in complaints, data authority investigations and audits, administrative fines, penalties or sanctions, seizure of equipment or data, civil actions (including class actions that have been introduced by Law No. 2016-1547 of 18 November 2016 for the Modernisation of the 21st Century Justice), criminal proceedings and private rights of action.

Proceedings

When the CNIL finds a PI owner to be in breach of its obligations under the LIL, as a preliminary step the CNIL chair may issue a formal notice for the PI owner to remedy the breach within a limited period. In cases of extreme urgency, this period may be reduced to 24 hours.

When the breach cannot be remedied in the context of a formal notice, the CNIL may impose one of the following sanctions without prior formal notice of adversarial procedure:

- a formal warning notification;
- a financial penalty; or
- the withdrawal of the authorisation to operate the data processing.

When the PI owner complies with the terms of the formal notice, the CNIL chair shall declare the proceedings closed. Otherwise, the competent committee of the CNIL may, after a contradictory procedure, pronounce one of the following penalties:

- a warning notification;
- a financial penalty, except when the PI owner is a public authority;
- an injunction to cease treatment; or
- the withdrawal of the authorisation granted by the CNIL for the data processing concerned.

In the case of emergency and infringement to civil rights and freedoms, the CNIL may, after an adversarial procedure, take the following measures:

- the suspension of the operation of data processing;
- a formal warning;
- the lockdown of PI for a maximum of three months (except for certain processing carried out on behalf of the French government); or
- for certain sensitive files of the French government, the prime minister is given information for him or her to take the necessary measures to remedy the breaches.

In the event of a serious and immediate violation of rights and freedoms, the chair of the CNIL may request, by summary application, the competent judge to order any necessary security measures.

The CNIL may also inform the public prosecutor that it has found infringements of data protection law that are criminally sanctionable.

Publicity of the penalties

The CNIL can make public the financial penalties that it pronounces. The inclusion of these sanctions in publications or newspapers is no longer subject to the bad-faith condition of the entity concerned.

Criminal sanctions

Infringements to data protection law may be punished by imprisonment for a maximum period of five years and a criminal fine up to €300,000 (articles 226-16 to 226-22-1 of the Criminal Code). However, criminal sanctions are hardly ever pronounced.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

An appeal may be lodged before the French Council of State against decisions made by the CNIL's restricted panel as well as formal notices issued by the CNIL's president.

This appeal must be lodged within two months of their notification (four months for an organisation located abroad).

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Law on Computer Technology and Freedom of 6 January 1978 (LIL) is generally applicable to all public bodies and all non-public entities that process PI and intends to cover all sectors. However, certain processing carried out by public authorities is subject to specific obligations that differ from the general obligations imposed upon private entities, for example:

- processing of PI by public bodies for reasons of national security is subject to a specific regime supervised by the executive power; and
- processing of PI managed by judicial authorities related to offences, convictions and security measures is subject to a specific regime supervised by the executive power.

The following categories of data processing fall outside the scope of the LIL:

- processing of PI solely for journalistic or artistic purposes; and
- processing of PI by a natural person in the course of a purely personal or household activity.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The LIL neither directly covers the interception of communications nor surveillance of individuals when implemented for public interest purposes.

This is subject to the authority of a dedicated public authority, the National Commission for Monitoring Intelligence Techniques. This field is regulated by several laws, mainly Law No. 91-646 of 10 July 1991 and Law No. 2015-912 of 24 July 2015.

Article 87 of the LIL states, however, that all 'processing of personal data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties' is only lawful if it complies with the provisions of articles 89 and 90 of the LIL, namely:

- if the processing concerns state security, defence or public safety or if its purpose is the prevention, investigation, recording or prosecution of criminal offences, it must be authorised by order of the competent minister after a reasoned opinion from the National Commission for Data Protection and Liberties (CNIL); and
- if the processing is of sensitive data as defined in article 6, I, of Law No. 78-17, it must also be authorised by a decree of the Council of State issued after a reasoned and published opinion from the CNIL, in which case the processing operations covered by these articles may concern the surveillance of data subjects.

On 12 January 2021, the CNIL's restricted committee sanctioned the French Ministry of the Interior for having illegally used drones equipped with cameras, in particular, to monitor compliance with containment measures related to the covid-19 pandemic. It also ordered the Ministry to cease all drone flights until a normative framework authorises it.

Although surveillance is not, as such, covered by the LIL, certain articles are applicable to regulate and secure such practices.

Law No. 2004-575 of 21 June 2004 for confidence in the digital economy established the principle of the prohibition of any direct prospecting by email, autodialler machines or faxes, carried out from the contact details of natural persons who have not expressed their prior consent to such messages.

These provisions concerning Electronic marketing have been included in the Postal and Electronic Communication Code (article L34-5 et seq) and in the Consumer Code (article L121-20-5 et seq).

In 2022, three priority themes have been chosen by the CNIL College, including the theme of 'monitoring telecommuters'. The use of telecommuting has been made compulsory by the various epidemic waves linked to covid-19. Many employees, agents and employers believe that it is going to become widespread and will continue, both in companies and in administrations, even when the health situation has returned to normal.

Although the CNIL has communicated the rules and good practices to be respected in such a context, it believes that it is necessary to ensure that employers' practices are compliant in the field.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Processing of health PI is subject to the provisions of the Public Health Code as well as to the LIL.

The solicitation by autodialler machine, email or fax, and the sale or transfer of PI for prospecting purposes using these, is subject to the provisions of the Postal and Electronic Communications Code.

PI formats

9 | What categories and types of PI are covered by the law?

The LIL is aimed at covering all forms of PI, which means any information relating to an individual who is identified or who could be directly or indirectly identified, by reference to an identification number or the combination of one or several elements.

Also, the LIL applies to automatic processing and to non-automatic processing of PI that forms part of a filing system (or is intended to form part of a filing system), except for processing carried out for

personal purposes. Accordingly, even records of PI in paper form may be subject to the LIL.

Finally, the LIL also distinguishes between data that could be called 'standard' (eg, identification and contact details, etc) and data that is also called sensitive or particular. The latter is subject to a prohibition on processing as a matter of principle unless the controller processing them justifies an exception formulated in article 9 of Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) and article 6 of the LIL.

Extraterritoriality

10 Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The LIL applies to the processing of PI carried out by a PI owner that is established in France, whether or not the processing takes place in France. In this context, 'establishment' is broadly interpreted as it refers to all sorts of 'installation', regardless of its legal form; or that is not established in France, but uses a means of processing located in French territory, for instance, hosting data, internet service provider and cloud services, among others. Therefore, the LIL has no extraterritorial effect.

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

In principle, the LIL applies to all processing of PI, except for that carried out for purely personal purposes. The controller determines the purposes for which and how PI is processed, whereas the processor processes PI only on behalf of the controller. The data controller must ensure that its processor complies with the GDPR. The duties of the processor towards the controller must be specified in a contract or another legal act.

In principle, the PI controller is the principal party for responsibilities such as collecting consent, enabling the right to access or managing consent-revoking. However, the GDPR introduces direct obligations for PI processors (including security, international transfers and record keeping, etc) and thus they can be held directly liable by data protection authorities for breaches of the GDPR and the LIL.

Controllers and processors are also jointly and severally liable where they are both responsible for damage caused by a breach.

On 27 January 2021, the CNIL's Restricted Section imposed penalties of €150,000 and €75,000 on a controller and its processor for not having taken satisfactory measures to deal with credential stuffing attacks on the controller's website.

This decision shows that although the controller must communicate documented instructions to its processor and decide on the implementation of security measures, the processor must also seek the most appropriate technical and organisational solutions to ensure the security of personal data, and propose them to the controller.

This decision, which is not public, must be considered as an alert. If the two actors have distinct obligations, this does not prevent them from developing a cooperative relationship to ensure the security of the data of the persons concerned.

The CNIL's restricted panel may also sentence a single actor in its capacity as data controller and data processor, depending on the non-compliance observed. This is the case of a payment service provider fined in December 2021 both in its quality of controller (security obligations and security breach) and in its quality of processor (non-compliance with the requirements of article 28 of the GDPR).

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Every collection, processing or use of PI needs to be justified under French data protection law. Like Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR), the Law on Computer Technology and Freedom of 6 January 1978 (LIL) lists six legal bases on which personal data can be processed, including:

- obtaining the prior consent of the data subject;
- the respect of a legal obligation of the data controller;
- the protection of the data subject's life (interpreted restrictively);
- the performance of a public service mission entrusted to the data controller or the data recipient;
- the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject before entering a contract; or
- the pursuit of the data controller's or the data recipient's legitimate interest provided such interest is not incompatible with the fundamental rights and interests of the data subject.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

French law is more restrictive for the processing of specific types of PI, known as sensitive personal data. As a matter of principle, the processing of sensitive data is prohibited.

The LIL provides a non-exhaustive list of sensitive PI by nature, which is PI that reveals, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of individuals, or that concerns their health or sexual life. This category of sensitive data by nature can only be processed in the following cases, among others:

- the data subject gave prior express consent;
- the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his or her consent;
- the processing is carried out by a foundation, association or any other non-profit organisation with political, philosophical, religious or trade union objectives, in the course of its legitimate activities;
- the processing relates to PI that has been made public by the data subject; or
- the processing is necessary for the establishment, exercise or defence of legal claims.

Concerning the use of PI in the employment context, the National Commission for Data Protection and Liberties published several opinions on monitoring the activities of employees, video surveillance, discrimination, localisation data and collection of PI in the recruitment process. Moreover, in France, employers cannot rely on consent for processing involving PI of its employees, since the employees cannot freely consent as they are by nature subordinated to the employer.

Moreover, processing can be prohibited due to its context, such as the processing of PI relating to offences, convictions and security measures, which can only be carried out by a limited number of specific entities.

Further, according to the law on the protection of personal data, a minor may consent to the processing of personal data alone

concerning the offer of information society services from the age of 15, which differs from the threshold of 16 years provided in the GDPR.

The law on the protection of personal data establishes a principle of prohibition of decisions producing legal effects on the sole basis of automated processing, including profiling intended to define the profile of the person concerned or to evaluate certain aspects of his or her personality. Such a provision maintains a certain gap with the GDPR since the law is based on a prohibition in principle of such automated processing while the GDPR refers to an 'individual right' of the person concerned 'not to be the subject of a decision based solely on automated processing, including profiling'.

Finally, it is necessary to recall that if the data controller outsources the hosting of health data, considered as sensitive, to a service provider, the latter must be an approved or certified host for such hosting under the provisions of article L1111-8 of the French Public Health Code.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

As a general rule, data subjects shall be provided with the following information when their PI is collected:

- the identity of the data controller;
- contact details for the data protection officer, where applicable;
- the purposes and the legal basis of the processing;
- the category of personal data;
- when PI is collected via a questionnaire, whether replies to the question are compulsory or optional;
- the consequences of an absence of reply;
- the categories of recipients of the data;
- information on the data subject's rights and the method to be used to exercise them (ie, the right to access the collected PI and to rectify, complete, update, block or delete it if inaccurate, incomplete, equivocal or expired; and the right to direct the use of their PI after their death);
- the intended transfer of PI outside the European Economic Area;
- the storage duration or the criteria that will be used to determine the duration;
- the right to lodge a complaint with a supervisory authority; and
- the existence of automated decision-making, including profiling and, if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the data subject.

Where the data was not obtained from the data subject, the information must be provided at the time of recording of the personal data or, if disclosure to a third party is planned, no later than at the time the data is disclosed for the first time.

When the data controller collects personal data from a minor under the age of 15, he or she must ensure that all such information is transmitted to the minor 'in clear and easily accessible language'.

To assist young people, parents and professionals in setting up a digital environment that is more respectful of children's interests, the CNIL published on 9 June 2021, eight recommendations to strengthen the protection of minors online.

Exemptions from transparency obligations

15 | When is notice not required?

In any case, notice is not required if the data subject already received such information. Further, in cases where the data subject did not provide his or her PI directly, the data controller is exempted from the notification obligation if:

- informing the data subject proves impossible or would involve a disproportionate effort, in particular in the context of statistical, historical or scientific research, or for the purpose of medical examination of the population to protect and promote public health;
- the PI is recorded only to comply with statutory and legal obligations; or
- the PI must remain confidential subject to an obligation of professional secrecy regulated by EU or EU member state law, including a statutory obligation of secrecy.

In the context of indirect data collection, the Law on Computer Technology and Freedom of 6 January 1978 (LIL) also specifies that the right to information does not apply:

- when processing is carried out on behalf of the state and is of interest to public security, insofar as such a limitation is necessary for the purposes of the processing and is provided for in the act establishing the processing; or
- when the processing is implemented by public administrations whose mission is either to control or recover taxes or to carry out controls on the activity of natural or legal persons that may lead to the detection of an infringement or failure to comply, to administrative fines or penalties.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

As a general rule, the PI controller shall ensure that the processed PI is adequate, relevant and not excessive concerning the purposes for which it is collected and for onward processing. Also, the PI owner shall ensure that PI is accurate, complete and, if necessary, updated. In this respect, the law provides that the PI owner shall take appropriate measures to ensure that inaccurate or incomplete data for the purposes for which it is collected or processed is erased or rectified.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

PI owners are required to limit the processing of PI to what is strictly necessary for the purpose of the processing. The amount of PI collected and processed must be proportionate to the purposes of the processing.

The LIL also provides that the PI must only be kept in a form enabling the data subject to be identified for a period that does not exceed the time necessary for the purposes for which the PI is collected and processed. Accordingly, if the legitimate ground of the processing has disappeared or expired, the controller should erase, anonymise or pseudonymise the PI.

The National Commission for Data Protection and Liberties (CNIL) distinguishes three life cycles for data:

- active storage: for the time necessary to achieve the objective or purpose of the initial processing;
- intermediate storage: the data is no longer necessary to achieve the set objective but is still of administrative interest or must be kept to meet a legal obligation. They will only be consulted on an ad hoc basis and by a limited number of people; and

- permanent archiving: because of their value or interest, the data may be permanently archived.

In certain cases, the retention period may be set by law (eg, article L3243-4 of the French Labour Code requires the employer to keep a duplicate of the employee's payslip for five years).

Outside of these cases, it is up to the person responsible for the file to determine the length of retention according to the purpose of the processing.

Data retention

18 Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

In accordance with the principles of the GDPR and the LIL, the CNIL indicates that personal data cannot be kept indefinitely.

A maximum retention period for the data collected must be determined by the data controller according to the purpose for which the data was collected.

The CNIL differentiates the retention of personal data based on several data life cycles:

- a retention in an 'active base' for the period necessary to pursue the purpose for which it is collected;
- an intermediate storage when the data is no longer used to reach the purpose, but is of administrative interest to the data controller; and
- a definitive archiving because of their value or interest. For this kind of storage, however, an evaluation of the necessity must be made on a case-by-case basis.

The retention periods may be set by law (labour code, commercial code) or, failing that, must be set by the data controller according to the purpose of the data processing.

To assist data controllers in identifying the relevant retention periods, the CNIL has developed tools to facilitate the implementation of this principle (practical guide, retention period guidelines according to sectors, etc).

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The finality principle is a core principle of data protection regulation in France. PI can only be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes.

Further, the CNIL already encourages PI controllers to implement the 'data minimisation' principle (which is enshrined in the GDPR), as well as the systematic use, where applicable, of anonymisation and pseudonymisation techniques.

Data originally collected for one purpose may be used for another purpose, but only in certain circumstances.

If the data controller has collected data on the basis of a legitimate interest, contract or vital interests, the data may be used for another purpose but only after verifying that the new purpose is compatible with the original purpose.

The data controller must, however, ensure that there is a link between the original purpose and the new or future purpose, the context in which the data were collected, the type and nature of the data, the possible consequences of the envisaged further processing or the existence of appropriate safeguards.

The compatibility test is not required if the data controller wishes to use the data for further statistical or scientific research purposes.

If the data controller has collected data on the basis of consent or in compliance with a legal requirement, no further processing is possible. It would require a new consent or a new legal basis.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Under the GDPR, data subjects have the right not to be subject to a fully automated decision that has a legal effect or significantly affects them, except with explicit consent, a decision necessary for the performance of a contract or as authorised by specific legal provisions.

The LIL prohibits that a judicial decision involving an assessment of a person's behaviour may be based on automated processing of personal data intended to assess certain aspects of that person's personality.

No decision producing legal effects on a person or significantly affecting him or her may be taken solely on the basis of automated processing of personal data, including profiling, with the exception of those mentioned in article 22.2 (a) and (c) of the GDPR or individual administrative decisions taken in compliance with article L 311-3-1 and Chapter I of Title I of Book IV of the French Code of Relations between the Public and the Administration.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Data controllers must protect PI against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves data transmission over networks.

Data controllers are required to take steps to:

- ensure that PI in their possession and control is protected from unauthorised access and use;
- implement appropriate physical, technical and organisational security safeguards to protect PI; and
- ensure that the level of security is appropriate with the amount, nature and sensitivity of the PI.

The National Commission for Data Protection and Liberties (CNIL) issued guidelines on 23 January 2018 on the security measures to be implemented by data controllers, in line with the requirement of Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR), to guarantee the security of personal data processing. These guidelines encourage data controllers to perform a privacy impact assessment, which shall be carried out in consideration of the two following pillars:

- the principles and fundamental rights identified as 'not negotiable', which are set by law and must be respected. They shall not be subject to any modulation, irrespective of the nature, seriousness or likelihood of the risks incurred; and
- the management of risks on data subjects that allows data controllers to determine which appropriate technical and organisational measures shall be taken to protect the PI.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

With the GDPR, there is a general obligation for PI controllers to report PI data breaches to the CNIL without undue delay and, where feasible, not later than 72 hours after becoming aware of it. However, an exception to this notification exists when the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is not made within 72 hours, reasons will have to be provided to the supervisory authority.

The notification shall 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 another 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 owner to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The CNIL considers that two conditions must be fulfilled to constitute a data breach within the meaning of the GDPR:

- a processing of personal data is implemented; and
- the personal data subject to the processing has been breached (ie, a security incident resulting in a loss of availability, integrity or confidentiality of personal data, either accidentally or unlawfully).

Moreover, when the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the controller shall notify the data breach to the data subject without undue delay. This notification can be waived if the CNIL considers that:

- the controller has taken subsequent measures that ensure the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- appropriate technical and organisational protection was in place at the time of the incident (eg, encrypted data); or
- the notification would trigger disproportionate efforts (instead, a public information campaign or 'similar measures' should be relied on so that affected data subjects can be effectively informed).

The Law on Computer Technology and Freedom of 6 January 1978 specifies that such notification is not required if the CNIL has found that appropriate safeguards have been implemented to render the data unintelligible to any person not authorised to access it and have been applied to the data affected by such breach.

The PI owner must keep an updated record of all PI breaches, which must contain the list of conditions, effects and measures taken as remedies. This record must be communicated to the CNIL on request.

Failure to meet the above requirements exposes the owners of PI to an administrative fine of up to €10 million or, in the case of an undertaking, up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Providers of electronic communication services are also subject to an obligation to notify the CNIL within 24 hours in the event of a PI breach. In this respect, when the PI breach may affect PI or the privacy of a data subject, the PI controller shall also notify the concerned data subject without delay.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

To meet the accountability obligation implemented by Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR), the CNIL indicates that each data controller must, to prove its compliance with the regulation, constitute and gather the documentation necessary for its compliance with the GDPR.

The CNIL also indicates that all actions and documents carried out at each stage of compliance must be reviewed and updated regularly to ensure ongoing compliance with the regulation.

This involves, in particular, the completion of a file including:

- documentation on the processing of personal data (record of processing activities, impact analysis and framework for transfers outside the European Union);
- documentation relating to information on the data subjects (information notices, models for collecting consent from the data subjects and procedures put in place for exercising rights); and
- documentation relating to contracts that define the roles and responsibilities of each of the actors (contracts with subcontractors, internal data breach procedures and proof of consent where applicable).

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Controllers and processors may decide to appoint a data protection officer (DPO). However, this is mandatory for public sector bodies, those involved in certain listed sensitive processing or monitoring activities or where local law requires an appointment to be made.

The DPO assists the owner or the processor in all issues relating to the protection of PI. Simply, the DPO must:

- monitor compliance of the organisation with all regulations regarding data protection, including audits, awareness-raising activities and training of staff involved in processing operations;
- advise and inform the owner or processor, as well as their employees, of their obligations under data protection regulations;
- act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights; and
- cooperate with the data protection authorities (DPAs) and act as a contact point for DPAs on issues relating to processing.

A single DPO may be appointed for several competent authorities, depending on their organisational structure and size.

The CNIL sets out the required skills that a DPO must have to be appointed:

- legal and technical expertise in the field of personal data protection; and
- a good knowledge of the business sector; of the internal organisation, in particular of the processing operations; of the information systems; and of the needs in terms of data protection and security.

However, the CNIL states that a prospective DPO can acquire all of these skills through appropriate training.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

PI controllers are required to maintain a record of processing activities under their responsibilities as referred to in article 30 of Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR). Processors of PI are also required to maintain such a record about personal data that controllers engage them to process.

While an exemption from the above obligations applies to organisations employing fewer than 250 people, this exemption will not apply where sensitive data is processed and where owners or processors of PI find themselves in the position of:

- carrying out processing likely to result in a risk (not just a high risk) to the rights of the data subjects;
- processing personal data on a non-occasional basis; or
- processing sensitive data or data relating to criminal convictions.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

According to article 35 of GDPR, PI controllers, in certain cases, are required to realise a data protection impact assessment (PIA). Thus, they are required to carry out a risk assessment in relation to certain use of PI.

The PI controllers must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where the envisaged processing is likely to result in a high risk to the rights and freedoms of natural persons.

The CNIL has published a list of processing operations for which a PIA is mandatory. In addition, a PIA must be realised where the operation meets at least two of the nine criteria of the G29 (ex-European Data Protection Board) Guidelines.

When a PIA is carried out, the risk assessment in relation to the envisaged processing must cover:

- a legal analysis, including:
  - the measures to ensure proportionality and necessity of the processing; and
  - the measures to ensures the rights of data subjects; and
- a data security analysis, including:
  - several scripts describing a feared event and all the threats that would allow it to occur to determine the risk level;
  - an evaluation of existing or planned measures to respond to a security breach; and
  - an assessment of the risks to the privacy of the data subjects.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Since the GDPR is directly effective in France, controllers and processors of PI are required to apply a privacy by design approach by implementing technical and organisational measures to show that they have considered and integrated data compliance measures into their data-processing activities. These technical and organisational measures might include the use of pseudonymisation techniques, staff training programmes and specific policies and procedures.

Also, when processing is likely to result in a high risk to the rights and freedoms of natural persons, owners and controllers are required to carry out a detailed PIA. Where a PIA results in the conclusion that there is indeed a high, and unmitigated, risk for the data subjects, controllers must notify the supervisory authority and obtain its view on the adequacy of the measures proposed by the PIA to reduce the risks of processing.

Controllers and processors may decide to appoint a DPO.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

PI controllers or processors are not required to register with the National Commission for Data Protection and Liberties (CNIL).

Since the entry into force of Regulation (EU) 2016/679 (General Data Protection Regulation), owners and processors no longer have the obligation to declare the PI processing they carry out to the CNIL.

However, the law on personal data maintains the requirement of prior authorisation from the CNIL for biometric or genetic data gathered by the state for research, and study or evaluation in the field of health.

In addition, and pursuant to article 37.7 of the GDPR, when a DPO is appointed, PI controllers or processors are required to designate him or her with the CNIL. This appointment can be made via the CNIL's website.

Other transparency duties

29 | Are there any other public transparency duties?

Not to our knowledge.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Under the Law on Computer Technology and Freedom of 6 January 1978 (LIL) regime, any person that processes PI on behalf of the data controller is regarded as a processor. The processor may only process PI under the data controller's instructions.

When a data controller outsources some of its processing or transfers PI concerning such processing to a sub-contractor (ie, a data processor), it must establish an agreement with that processor.

This agreement must specify the obligations incumbent upon the processor as regards the obligation of protection of the security and confidentiality of the data and provide that the processor may act only upon the instruction of the data controller. If data transfers occur with this processor outside the European Union, the CNIL refers to the standard contracts between controllers and processors adopted by the European Commission on 4 June 2021.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Generally, there are no specific restrictions on the disclosure of PI other than the general data protection principles provided by the LIL.

Moreover, in the case of data covered by professional secrecy, the person in charge must ensure, before any disclosure, that it is possible to transfer such data (authorisation, organisation benefiting from a specific legislative provision).

Nevertheless, disclosure of sensitive PI such as health data is limited to certain institutions and professionals, unless the data

controller has obtained a specific and express consent of the data subject for the disclosure of such PI.

Regarding the sale and transmission of the personal data of customers or prospects to business partners who wish to use them for commercial prospecting purposes:

- by mail or telephone call: the data subjects must be informed and given the opportunity to oppose the transmission of their data in a simple and free manner; and
- by electronic means (email, SMS, etc): the organisation transmitting the data must obtain the consent of the data subjects for this transmission. The data subjects must also be informed of this transfer and of the identity of the business partners on whose behalf the consent is collected and of the purposes for which the data will be used.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

PI can be transferred freely to other countries within the European Economic Area, as well as to countries recognised by the European Commission as providing an 'adequate level of data protection'.

Such transfers of PI from France are permitted to Canada (under certain conditions), Andorra, Argentina, Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, Switzerland, Uruguay and New Zealand.

A controller or processor may transfer PI to other countries only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The appropriate safeguards may be provided for by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules approved by the National Commission for Data Protection and Liberties (CNIL);
- standard data protection clauses – model clauses designed by the European Commission to facilitate transfers of personal data from the European Union to all third countries, while providing sufficient safeguards for the protection of individuals' privacy;
- a code of conduct approved by the CNIL, 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
- a certification mechanism approved by the CNIL 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.

Subject to CNIL authorisation, the appropriate safeguards may also be provided for, in particular, by:

- 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
- provisions to be inserted into administrative arrangements between public authorities or bodies, which include enforceable and effective data subject rights.

However, in the absence of an adequacy decision or of appropriate safeguards as mentioned earlier, a transfer of personal data to a third country or an international organisation shall take place if:

- the data subject has explicitly consented to its transfer after having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or
- the transfer is necessary under one of the following conditions:
    - protection of the data subject's life;
    - protection of the public interest;
    - to meet obligations ensuring the establishment, exercise or defence of legal claims;
    - consultation of a public register that is intended for public information and is open for public consultation or by any person demonstrating a legitimate interest;
    - performance of a contract between the data controller and the data subject, or precontractual measures taken in response to the data subject's request; or
    - conclusion or performance of a contract, either concluded or to be concluded in the interest of the data subject between the data controller and a third party.

Data controllers must inform data subjects of the data transfer and provide the following information:

- the country where the data recipient is established;
- the nature of the data transferred;
- the purpose of the transfer;
- categories of the recipients;
- the level of protection of the state concerned or adopted alternative measures; and
- the means by which to obtain a copy of the appropriate or suitable safeguards and where they have been made available.

On 16 July 2020, the Court of Justice of the European Union invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU–US Data Privacy Shield framework (Case C-311/18). There is no transitional period.

The Privacy Shield was implemented to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States.

As a result, all internationally active companies in the European Union should closely review their data transfers to the US and examine whether they can carry out their data transfers to the US based on other mechanisms, such as the EU's standard contractual clauses (SCCs).

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Restrictions on cross-border transfers apply to transfers from the PI owner based in France to a data processor outside the European Economic Area. Onward transfers are in principle subject to the restrictions in force in the recipient's jurisdiction. By exception, SCCs contain specific requirements for onward transfers.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

Not applicable.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Data subjects have a right to 'access' the PI that a controller holds about them.

Data subjects can exercise their right of access by sending a signed and dated access request, together with proof of identity. Data subjects can request that the PI owner provides the following information:

- confirmation as to whether the controller processes the data subject's PI;
- information related to the purposes for which the PI is processed, and the recipients or categories of recipients to whom the PI is or has been provided;
- where applicable, information related to cross-border data transfers;
- the logic involved in any automated decision making (if any);
- the communication, in an accessible form, of personal data concerning the data subject as well as any information available as to the origin of the data;
- information allowing the data subject to know and to contest the logic underlying the automated processing in the event of a decision taken based on it and producing legal effects concerning the person concerned;
- the envisaged duration of the processing or the criteria for determining the duration; and
- any available information on the source of the data, if not collected from the data subject.

The controller may oppose manifestly abusive access requests, in particular concerning their excessive number or repetitive or systematic nature. In the event of a claim from the data subject, the burden of proving the manifestly abusive nature of the requests lies with the PI owner to whom they are addressed.

The right of access may be denied when the personal data is kept in a form that excludes any risk of invasion of the privacy of the data subjects (ie, if PI is pseudonymised or anonymised) and for a period not exceeding what is necessary for the sole purpose of statistical, scientific or historical research.

According to article 15 (4) of the Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR), the right of access may also be denied when data subject's access request affects the rights and freedoms of others.

Other rights

36 | Do individuals have other substantive rights?

Also to the right of access described above, data subjects are granted the rights described below. When PI has been collected by electronic means, the data subjects must be provided with a way to exercise their rights using electronic means.

Right to object

Data subjects have the right to object to the processing of their PI on legitimate grounds unless the processing is necessary for compliance with a legal obligation or when the act authorising the processing expressly excludes the data subjects' right to object.

Data subjects also have the right to object, at no fee and without justification, to the use of PI related to them for the purposes of direct marketing by the PI owner or by an onward data controller.

Right to correct

Upon proof of their identity, data subjects may require the PI owner to correct, supplement, update, lock or erase personal data related to them that is inaccurate, incomplete, equivocal or out of date, or whose collection, use, disclosure or storage is prohibited.

When the concerned PI has been transmitted to a third party, the data controller must carry out the necessary diligence to notify such a third party of the modifications operated following the data subjects' request.

Right to be forgotten

Data subjects have the right to request the PI controller to erase personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, in particular where one of the following grounds applies:

- the PI is no longer necessary concerning the purposes for which it was collected or otherwise processed;
- the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- the PI has been unlawfully processed;
- the PI has to be erased for compliance with a legal obligation in EU or EU member state law to which the controller is subject; or
- the PI has been collected concerning the offer of information society services.

On 27 March 2020, the Council of State issued a ruling on the right to be forgotten, which marks the end of a legal battle between the National Commission for Data Protection and Liberties (CNIL) and Google regarding the territorial scope of the right to be forgotten under EU law.

The CNIL originally fined Google €100,000. According to the CNIL, Google's practice was to only remove references on EU versions of its search engine following a request thereto (thus, only blocking the results in the EU-specific versions). For the CNIL, only the global removal of search results could ensure the effective protection of individuals' rights.

Following this sanction, Google filed an appeal before the Council of State because the 'right to be forgotten', as it is currently established under EU data protection law is limited to the territory of the European Union and Google, therefore, cannot be forced to remove the search results globally on all its domain names extensions.

The Council of State, noting 'several serious difficulties regarding the interpretation of the directive', subsequently referred questions to the Court of Justice of the European Union (CJEU) for a preliminary ruling concerning the scope of the right to be forgotten.

Taking the side of Google, the CJEU in *Google v CNIL* (Case C-507/17) held that the scope of de-referencing only applies for results of a search carried out from within EU territory. Therefore, the results will still be accessible if a search is performed outside the European Union.

Although the CJEU ruled that the 'right to be forgotten' does not apply at a global scale, it clearly stated that the de-referencing must be effective at EU scale, and not only in the local version of the search engine found in the country where the individual concerned lives.

Moreover, the CJEU specifies that, although there is no obligation of global de-referencing under EU law, it is also not forbidden. Thus, a supervisory authority, and so the CNIL, has the authority to force a search engine operator to delist results on all the versions of the search engine if it is justified in some cases to guarantee the rights of the individuals concerned.

Finally, the court demanded that search engine operators take efficient measures to prevent or, at the very least, seriously discourage an internet user from gaining access to delisted links.

Following the CJEU's decision of 27 March 2020, the Council of State annulled the CNIL sanction on Google.

The Council of State ruled that the CNIL was not entitled to order a worldwide delisting. As a result, the sanction did not rely on an appropriate legal ground and that there is currently no legislative provision in France that suggests that the right to dereferencing could apply outside the territory of the European Union. The Council of State also pointed out that, in any case, the right to global de-referencing would only have been permitted if the CNIL had struck a balance between the individual's right to privacy and the general public's right to freedom of information, which the CNIL had failed to do when it sanctioned Google.

Right to be forgotten for children

Data subjects have the right to request the PI controller to erase without undue delay the personal data that has been collected in the context of the provision of information society services where the data subject was underage at the time of collection. When the PI controller has transmitted the concerned data to another PI owner, the data controller shall take reasonable measures, including technical measures, to inform the onward PI owner of the data subject's request for the deletion of any link to the data, or any copy or reproduction thereof.

This is unless the data processing is necessary:

- to exercise the right to freedom of expression and information;
- to comply with a legal obligation requiring the processing of such data or to carry out a task in the public interest or the exercise of the public authority entrusted to the controller;
- for public health;
- for archival purposes of public interest, for scientific or historical research or statistical purposes; or
- to establish or exercise legal rights.

Right of data portability

Data subjects have a right to:

- receive a copy of their personal data in a structured, commonly used, machine-readable format that supports re-use;
- transfer their personal data from one controller to another;
- store their personal data for further personal use on a private device; and
- have their personal data transmitted directly between controllers without hindrance.

Digital death

Data subjects have the right to set guidelines for the retention, deletion and communication of their personal data after their death.

In a press release of 28 October 2020, the CNIL identified that every day, nearly 8,000 Facebook accounts were left abandoned following the death of their owners and wondered what solutions could be brought to this problem. To raise awareness on the subject, it has therefore published guidelines on digital death and the fate of a deceased person's data.

Automated individual decision-making, including profiling

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 him or her or similarly significantly affects him or her, unless it is:

- necessary for entering into, or performance of, a contract between the data subject and a data controller;
- authorised by EU or EU member state law to which the controller is subject and that 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.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals may claim for damages when they are affected by a breach of the Law on Computer Technology and Freedom of 6 January 1978 (LIL) that qualifies as a criminal offence subject to the referral to criminal jurisdiction.

Also, the LIL allows under certain conditions, when several natural persons placed in a similar situation suffer damage having as a common cause a breach of the same nature of the requirements of the LIL or GDPR by a personal data controller or processor, that a group action be brought before the civil court or the competent administrative court given the individual cases presented by the claimant, who shall inform the CNIL.

In this case, compensation may amount to the total amount of damage endured by the individual, which includes moral damages or injury to feelings.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Where the data controller does not answer or refuses to grant the right to the data subjects' request, the latter can refer to the CNIL or a judge to obtain interim measures against the data controller.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Not applicable.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Data controllers may install cookies or equivalent devices subject to the data subject's prior consent.

In July 2019, the National Commission for Data Protection and Liberties (CNIL) issued new guidelines about the use of cookies that are also supplemented by two decisions rendered by the Council of State on 6 June 2018 (No. 412589 – as to means of blocking the placement of cookies) and by the Court of Justice of the European Union on 1 October 2019 (C-673/17 – as to the data subject's consent). These guidelines are intended to provide reminders of the French rules that apply to the use of cookies and similar technologies in the light of the strengthened consent requirements under Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR).

These guidelines were followed by draft recommendations that complete the guidelines by providing concrete advice on good practice and practical examples of measures to comply with the requirements of the French legal framework applicable to cookies.

The Council of State ruled on 19 June 2020 to remove one of the parts of these lines that prohibited the 'cookie wall', stating that: 'In particular, the CNIL believed that access to a website could never be conditional on the acceptance of cookies'.

The Council of State censured this section, considering that the commission had 'exceeded what it can legally do, within the framework of a flexible law instrument'.

On 17 September 2020, the CNIL adopted two documents dealing with cookies, repealing those of 4 July 2019, and supplemented by a recommendation 'proposing practical methods of compliance when using cookies and other tracers. Non-prescriptive and non-exhaustive' tracks following a public consultation.

These guidelines were published on 1 October 2020 and became effective on 1 April 2021. They confirm certain major principles.

At first, simply continuing to browse a site can no longer be considered a valid expression of consent.

Consent is required for all cookies other than those necessary for the use of the website or app, whether they are used in 'logged' or 'unlogged environments', and whether they are implemented by the website or app operator or a third party.

Notably, the following categories of cookies require the prior consent of the data subject:

- cookies related to targeted advertising;
- social networks' cookies generated in particular by their buttons of sharing when collecting personal data without the consent of the persons concerned; and
- analytics cookies.

Regarding analytics, the CNIL considers that these cookies may be exempted from prior consent where the following criteria are fulfilled:

- they must be implemented by the website operator or its subcontractor;
- the data subject must be informed before their implementation;
- it must be able to oppose it through an opposition mechanism that can be easily used on all devices, operating systems, applications and web browsers. No reading or writing operations must take place on the device from which the data subject objected;
- the purpose of the system must be limited to:
    - audience measurement of the content viewed to allow the evaluation of published content and the ergonomics of the site or application;
    - segmentation of the website audience into categories to evaluate the effectiveness of editorial choices, without this leading to targeting a single person; or
    - dynamic modification of a site in a global way;
- the personal data collected must not be combined with other processing operations (customer files or statistics on visits to other sites, for example) or transmitted to third parties. The use of cookies must also be strictly limited to the production of anonymous statistics. Its scope must be limited to a single site or mobile application editor and must not allow the tracking of the person's navigation using different applications or browsing different websites;
- the use of the IP address to geolocate the Internet user must not provide more accurate information than the city. The collected IP address must also be deleted or anonymised once the geolocation has been completed; and
- the cookies used by these processing operations shall not have a lifetime exceeding 13 months and this duration shall not be automatically extended upon new visits. The information collected through the cookies shall be retained for a maximum of 25 months.

The consent must be freely given, specific, informed and unambiguous.

Informed

Before collecting consent, PI owners must ensure that proper information has been provided to users.

The first layer of information is recommended to provide details about:

- the purposes of the cookies (eg, targeted or personalised advertising, non-personalised advertising, social media sharing, audience measurement or analytics);
- the list of data controllers who have access to the cookies (and associated data), which should be permanently accessible and regularly updated. The CNIL suggests that consent should be re-sought if the list changes materially (from a qualitative or quantitative perspective);
- whether a user's consent is also valid for tracking his or her navigation throughout other websites or apps (and which ones); and
- the right to withdraw consent at any time and how.

To avoid affecting the user experience, the CNIL suggests that details of the purposes for which cookies will be used could be provided to users in a layered fashion, for example via links or drop-down menus.

Freely given

Users must be offered a real choice between accepting or refusing cookies through two checkboxes or buttons – for example, 'accept' and 'refuse' – or equivalents, such as 'on' and 'off' sliders that should be deactivated by default and not be exposed to negative consequences should they decide to refuse cookies, which is in line with GDPR requirements.

Users must be able to consent or withhold their consent with the same degree of simplicity. This implies that the checkboxes, buttons or sliders should be of the same format and presented at the same level.

A 'cross' button should be inserted to allow users to close the consent interface, and not to make a choice. In that case, no cookies should be placed on the user's equipment. Users should then be asked again to choose between acceptance or refusal until a choice is made. In practice, this approach would require PI owners to record a third alternative (ie, no choice expressed by the user), and to seek consent again at a later stage.

In the case that the user refuses to consent to the use of cookies, his or her consent will not have to be sought again for a certain period. The CNIL considers that this period must be identical to the duration for which the consent would have been recorded.

The CNIL also considers that browsers do not, to date, make it possible to distinguish between trackers according to their purpose, even though this distinction may be necessary to guarantee the freedom of consent.

On 31 December 2021, the CNIL's restricted panel fined Facebook Ireland Limited €60 million because users of the social network facebook.com residing in France are not allowed to refuse cookies as easily as to accept them (decision SAN-2021-024).

Specific

The consent of the users should be collected for each type or category of cookies. However, the CNIL acknowledges that users can validly consent to all the purposes at once without preventing consent being specific, subject to the following conditions:

- all the purposes must have been explained to the user before his or her consent;
- the user is offered the option to consent for each individual purpose; and
- an option to refuse all the cookies globally is also provided to the user, in the same manner as the option to consent globally to all purposes at once.

Unambiguous

Implied consent is now prohibited, meaning that continuing to browse the website is no longer deemed to imply consent by the data subjects. A positive action of the data subject is now required. To address this, pre-ticked boxes or pre-slid toggles should be avoided.

Duration of the validity of consent

The CNIL recommends that consent is renewed at regular intervals, depending on the context and extent of the initial consent as well as the user's expectations. The CNIL considers that a period of six months would be appropriate.

In parallel, the CNIL also considers that the lifespan of a cookie cannot exceed 13 months. This means that two time factors should be considered: the cookie's lifespan and the time that has elapsed since consent was granted by the user.

Demonstrating consent

Data controllers should be able to provide individual evidence of users' consent, and evidence that their consent mechanism allows the gathering of valid consent.

The CNIL's recommendation suggests the following solutions:

- taking screenshots of the mechanism displayed for collecting consent as it appears on the relevant website or application;
- keeping in escrow with a third-party depositary the computer code used by the controller for collecting users' consent; and
- carrying out regular audits of the consent mechanisms implemented on the sites or apps where consent is sought.

In our view, the more economical and resource-effective solution is for the PI owners to take a screenshot of the visual aspect of the consent mechanism in place for each version of the website or application and to keep a copy on file, rather than opting for the escrow or audit approach, which would be costlier. However, PI owners will also need to keep a record of the consent received, consequently, audits are likely unavoidable in practice.

On 17 September 2020, the final version of the recommendations were adopted. The CNIL started inspections to enforce these recommendations on April 2021 and has already announced several sanctions against different controllers.

For example, on 31 December 2021, the CNIL fined Google for a total of €150 million (€90 million for Google LLC and € 60 million for Google Ireland Limited) since users of google.fr and youtube.com were not allowed to refuse cookies as easily as to accept them (decision SAN-2021-023). On 7 December 2020, in addition to fining them, the CNIL's restricted panel enjoined Google LLC and Google Ireland Limited, within three months, to inform the data subjects in advance and in a clear and complete manner, for example, on the information banner on the home page of google.fr, of:

- the purposes of all cookies subject to consent; and
- the means available to them to refuse them.

In view of the answers provided by Google LLC and Google Ireland Limited within the time limit set and considering that they have complied with the injunction it had issued, the restricted panel decided to close the procedure on 30 April 2021 (decision SAN-2021-004).

In a decision dated 28 January 2022, the Council of State confirmed the competence of the CNIL to impose sanctions on cookies outside the one-stop shop mechanism (CE 28-1-2022 No. 449209).

In addition, pending legislation or a position of the Court of Justice of the European Union regarding the 'cookie wall', the CNIL published on its website on 15 May 2022, criteria for assessing the lawfulness of this practice. These criteria include the following:

- a fair alternative for the user to access the content if he or she refuses to accept the cookies; and
- reasonable financial compensation in the case of a paid alternative.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Sending unsolicited marketing messages is prohibited without the prior consent of the recipient. Such consent of the data subject cannot derive from a pre-ticked box or a general acceptance of terms and conditions.

Under the following conditions, the prior consent of the data subject is not required to address unsolicited marketing messages:

- when the information of the data subject has been collected on the occasion of a purchase following the applicable data protection rules;
- the marketing messages concern products or services similar to those purchased by the data subject; and
- the data subject is provided with an easy way to opt-out of receiving marketing messages when the data is collected and with each marketing message.

In a business-to-business relationship, the prior consent of the recipient is not required provided that:

- the recipient has been informed that his or her email address would be used to address marketing messages;
- the recipient can oppose the use of his or her email address for the purpose of direct marketing at the time of its collection and with each message; and
- the marketing messages must be concerning the recipient's profession.

Direct marketing by regular mail, telephone or electronic channels is not subject to the prior consent of the recipient, but the recipient can object to it by signing up to an opt-out list. In France, this list is called Bloctel, which is the governmental opt-out list for telephone marketing.

Targeted advertising

42 | Are there any rules on targeted online advertising?

Advertising targeting is one of the main concerns of the CNIL, and it drew up an action plan for 2019–2020 to clarify the applicable rules and to support players in their compliance.

On the issue of commercial prospecting and partner opt-in, the CNIL has communicated the applicable rules of law on its website (commercial prospecting by email).

On the issue of cookies and tracers, the CNIL has updated its recommendations to align them with the European Data Protection Board (EDPB) Guidelines on consent.

On 13 April 2021, the EDPB adopted Guidelines 8/2020 on the targeting of social media users. These Guidelines offer guidance regarding the targeting of social media users, in particular as regards the responsibilities of targeters and social media providers.

There are no specific rules on targeted online advertising. However, the GDPR is fully applicable such as the Law on Computer Technology and Freedom of 6 January 1978 (LIL).

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Sensitive data is listed in article 6 of LIL. This is personal data that discloses the alleged racial or ethnic origin, political opinions, religious

or philosophical beliefs or trade union membership of a natural person or processed genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sexual life or sexual orientation of a natural person.

Regarding their processing, LIL refers to article 9 of the GDPR, which indicates that the processing of sensitive categories of personal information shall be prohibited except if:

- the data subject has given explicit consent to the processing;
- the 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 and social security and social protection law;
- the 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;
- the 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;
- the processing relates to personal data that is manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest.

The CNIL does not consider information relating to offences or convictions sensitive data, but it is subject to the same protection. Only the courts and certain public authorities can use it, as well as the victimised legal entity in the context of defending its interests.

In addition, the CNIL is dealing with the issue of the social security number (NIR) allocated to each individual at birth on the basis of civil status data. Insofar as it is unique to each person, particularly identifying and meaningful, its use presents a risk of population registration and ever-increasing file reconciliation. Therefore, the use of the NIR is strictly regulated by law. Its use is essentially limited to the health, social and work spheres and must systematically be subject to prior authorisation by the CNIL.

Profiling

44 | Are there any rules regarding individual profiling?

Article 95 of the LIL prohibits any profiling that results in discrimination against natural persons on the basis of the special categories of personal data mentioned in article 6 of the same law.

Moreover, article 47 of the LIL states that no decision producing legal effects on a natural person or significantly affecting him or her may be taken solely on the basis of automated processing of personal data, including profiling, except for the exceptions listed in the texts, and in particular those of article 22 of the GDPR.

The GDPR sets out the rules applicable to profiling and fully automated decisions. Moreover, guidelines have been adopted by all European CNILs to clarify and illustrate this new legal framework with concrete examples (Guidelines on Automated individual decision-making and Profiling).

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 him or her or similarly significantly affects him or her.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There is no specific provision applicable to cloud computing in the LIL or the GDPR. The CNIL issued guidelines addressed to companies contemplating subscription to cloud computing services on 25 June 2012. These guidelines contain seven recommendations by the CNIL that should be considered by data controllers when assessing the opportunity to migrate to cloud services, as well as a template clause to be inserted into agreements with cloud computing services providers.

The recommendations are to:

- establish a precise mapping of the data and processing that will be migrating to the cloud and the related risks;
- define technical and legal security requirements adapted to the categories of data and processing;
- carry out a risk analysis to identify the security measures to be implemented to preserve the essential interests of the company;
- identify the type of cloud services and data hosting appropriate concerning all data processing;
- select cloud service providers that provide adequate security and confidentiality guarantees;
- review and adapt the internal security policies of the company; and
- carry out regular assessments of the cloud services.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Following the outbreak of covid-19 and its development into a global pandemic, some questions arise about the development of apps to help manage the epidemic. Among these questions is the relevance and legality of the use of technologies for tracking and tracing individuals for the purpose of preventing the spread of the virus, both in employment context, for employers concerning their employees, and public context as part of the security mission of the public authorities.

In France, the Labour Code requires employers to implement measures necessary to ensure the security of the employee. At this regard, employers may implement third-party apps to do health screening, analyse travel records, etc.

The National Commission for Data Protection and Liberties (CNIL) sets the limits that must not be crossed 'the privacy-invasive measures of the data subjects, in particular through the collection of data that would go beyond the management of suspicions of exposure to the virus are prohibited'.

When implementing these measures, employers must consider the following key issues.

In the context of this pandemic, decisions have also been rendered, reflecting the *Schrems* decision on the invalidation of the privacy shield. Indeed, owing to the fear of possible transfers of personal data to the United States, associations and unions had asked the judge of the Council of State to suspend the Health Data Hub platform as a matter of urgency. This request was refused because the processing of data by Microsoft on the territory of the European Union was not in itself a serious and manifest illegality. This remains a sensitive issue at a time when platforms processing health data are multiplying in this crisis context (Council of State decision of the judge of summary proceedings of 13 October 2002).

Employers must have an appropriate legal basis for processing the personal data collected from individuals relating to the covid-19 outbreak

Employers may be tempted to collect as much information as possible from individuals relating to the covid-19 outbreak. A large proportion of this information will fall within the categories of 'personal data' and 'special categories of personal data'. Employers must rely on a legal basis provided for in article 6 of the General Data Protection Regulation (GDPR) when processing such data. In the context of covid-19, the legal basis could be compliance with a legal obligation. In France, the processing of health data by an employer must be authorised by a special text and not by a general provision such as that of ensuring the safety of the employee (article L4121-1 of the French Labour Code).

Employers should ensure that the purposes for which the data are collected and processed are well defined, explicit and legitimate

The GDPR requires that data controller only collect as much personal data as is strictly necessary for the purposes being pursued. Also, the choice to adopt a broad purpose to justify several processing is not possible. For example, nothing would justify an employer processing 'blood group' data for the implementation of preventive actions.

Review and update privacy policies as necessary

If an employer is collecting new categories of personal data from employees and processing such data for new purposes, it will likely be necessary to update privacy policies to reflect the new changes in the collection of data from employees. This principle is also provided for in the article L1222-4 of the French Labour Code, which states that:

> *No information concerning an employee personally may not be collected by a device that has not been worn prior to its knowledge. Moreover, employee representative bodies must be informed and consulted, when employers intend to introduce new technologies processing employees personal data.*

Employers should conduct a data protection impact assessment before collecting any personal data relating to the covid-19 outbreak

A data protection impact assessment (DPIA) is intended to help employers understand the risks associated with particular data processing activities and the measures that can be taken to mitigate such risks. Also, a DPIA may help the employers to target the amendments may be required in other data protection-related compliance documentation within the organisation (eg, privacy policies or records of processing activities). Additionally, guidance issued by CNIL suggests that a DPIA should be performed where a processing activity involves biometric data, genetic data or tracking data.

Regarding public authorities, the European Union and many member states have been putting forward various digital tracking measures aimed at mapping, monitoring and mitigating the pandemic. Such apps aim to alert people who have been in proximity to an infected person for a certain time, including those one may not notice or remember, without tracking the user's location.

On 16 April 2020, the European commission in cooperation with member states, European Data Protection Supervisor and the European Data Protection Board published guidelines aimed at ensuring that any covid-19 related apps fully comply with data protection standard and limiting intrusiveness.

In France, the government developed the application called StopCovid, which is designed to alert its users that they have been in close proximity to people who have been tested positive for covid-19 and who use the same application. The application is based on a voluntary use and allows contact tracing, using Bluetooth technology, without geolocating individuals. It is therefore alerting people who are using the application and who have been exposed to the risk of contamination.

CNIL was consulted by the Secretary of State for Digital Affairs on the compliance of the StopCovid app with the French data protection regulation. CNIL considered the system to be compliant with the GDPR, if certain conditions are met. It notes that a number of safeguards are provided by the government's plan, including the use of pseudonyms.

CNIL considered that the application can be deployed, in compliance with the GDPR, if its usefulness for crisis management is sufficiently proven and if certain safeguards are provided. In particular, its use must be temporary and the data must be kept for a limited period of time. CNIL therefore recommended that the impact of the system on the health situation be studied and documented on a regular basis, to help the public authorities decide whether or not to maintain it.

In its opinion, CNIL points out that the use of contact tracing applications must be part of a global health strategy and calls, in this respect, for particular vigilance against the temptation of 'technological solutionism'. It stresses that the app's effectiveness will depend, in particular, on its availability in application stores, widespread adoption by the public and appropriate configuration.

The StopCovid app was launched on June 2020.

Dark patterns on cookies banners

'Dark patterns' are deceptive user interfaces, carefully designed to make users make choices that they are not aware of or that they don't want to make. These practices are classified into four categories by the CNIL from the point of view of data protection, for which different design tactics can be implemented: take advantage, seduce, lure, complicate and prohibit. In its deliberation in September 2020, regarding the adoption of a recommendation proposing practical modalities of compliance in the event of the use of cookies and other tracers, and in order to not mislead users, the CNIL recommended that data controllers ensure that choice collection interfaces do not incorporate potentially misleading design practices that lead users to believe that their consent is mandatory or that visually emphasise one choice over another. It is recommended that buttons and fonts be the same size, easy to read and highlighted in the same way. The CNIL recalled these recommendations in the Q&A on 'CNIL's Amending Guidelines and Recommendation on Cookies and Other Tracers' that it published on 4 May 2022. Since May

Benjamin May
may@aramis-law.com

Marianne Long
long@aramis-law.com

9 rue Scribe
75009 Paris
France
Tel: +33 1 53 30 77 00
Fax: +33 1 53 30 77 01
www.aramis-law.com

2021, about 60 organisations that do not allow internet users to refuse cookies as easily as to accept them have been put on notice by the CNIL.

CNIL publishes a new white paper on payment data and means of payment

To raise awareness to the public, support professionals and anticipate future transformations, the CNIL has published a new white paper: 'When trust pays off: today's and tomorrow's means of payment methods facing the challenge of data protection'. This white paper raises a number of issues regarding the processing of payment data and the associated risks (traceability of the behaviour of the persons concerned) and highlights the sensitive subjects in this sector: the anonymity of transactions, international data transfers and legal security.

Germany

Peter Huppertz

Hoffmann Liebs Partnerschaft von Rechtsanwälten mbB

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Data protection in Germany is primarily governed by Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) that entered into force on 25 May 2018 as standardised EU law. However, as the GDPR includes specific opening clauses and allows national legislators an individual set of rules for particular areas via these clauses, Germany has its own national data protection law. Such national data protection law, for instance, data protection in the context of employment, is governed by the Federal Data Protection Act (the Act).

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

Overseeing the principles of data protection law is assigned to the individual federal states in Germany. Thus, every state has its own data protection authority (DPA), which is responsible for data processing in its territory.

The DPA can request any information that is necessary to audit compliance with the applicable data protection law and can further institute an investigatory (on-site) audit. To enforce these measures, the DPA may issue a warning or, alternatively, apply administrative measures of constraint, such as an injunction to take measures to guarantee compliance with statutory obligations or impose an order to stop illegal data processing. If the person does not provide the requested information to the DPA in time or does not duly cooperate in the DPA's audit measures, the DPA may issue a fine with an administrative financial penalty (up to €20 million or 4 per cent of annual turnover for the preceding fiscal year).

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The DPAs of the German federal states regularly meet as the Data Protection Conference and publish concerted opinions on controversial issues. EU DPAs have a similar association in the form of the European Data Protection Board (EDPB), which replaced the Article 29 Working Party. The EDPB publishes concerted opinions regularly as well. The GDPR further provides for a one-stop shop, allowing data controllers to coordinate cross-border processing activities in the European Union with only one leading DPA.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Serious breaches are punished by imprisonment for a maximum period of three years. Such offences are prosecuted only if a formal complaint is filed by the DPA, the affected data subject or the responsible data controller itself. Besides criminal sanctions of the Act, controllers may also be punished for disclosing or transmitting personal, company or business-related secrets to third persons under the terms of the German Criminal Code (violation of private secrecy) or the German Code Against Unfair Competition (violation of business secrecy).

Breaches may also incur fines. The GDPR provides for graduated breaches in this regard. There are three types of breaches:

- minor breaches with no administrative financial penalty;
- moderate breaches with an administrative financial penalty of up to €10 million or 2 per cent of annual turnover; and
- serious breaches with an administrative financial penalty of up to €20 million or 4 per cent of annual turnover.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Supervisory authorities are only allowed to exercise their extensive powers over controllers under the GDPR subject to appropriate safeguards, including effective judicial remedies and due process. Therefore, the GDPR provides data subjects with effective judicial redress in disputes with supervisory authorities. The administrative courts are responsible for this, although the ordinary courts have jurisdiction over proceedings for fines.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) is generally applicable to all federal public authorities, state public authorities and all non-public entities that process PI. However, the GDPR is subsidiary to various area-specific rules, which make several authorities or entities subject to special regulations.

Interception of communications and surveillance laws

7 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The GDPR does not cover interception of communications, which is addressed in other special regulations such as the German Code of Criminal Procedure (StPO), the German Code of Telecommunications (TKG) and the German Telecommunications-Telemedia Data Protection Act (TTDSG). Electronic marketing is covered only partially by the GDPR. The German Code Against Unfair Competition holds additional and more comprehensive provisions regarding this. Monitoring and surveillance of individuals are also covered by the StPO. In this regard, it is complemented by corresponding acts on the police authorities of the individual federal states.

Other laws

8 Are there any further laws or regulations that provide specific data protection rules for related areas?

There are dozens of area-specific rules on data privacy. Therefore, it is impossible to present every regulation with concern to data privacy in this context. But for this chapter's purposes, the TTDSG is worth noting because it provides comprehensive area-specific rules on telecommunication services.

PI formats

9 What categories and types of PI are covered by the law?

The GDPR shows no significant limitations to the scope of PI. Practically all data that provides information about personal or factual relationships of an identified or at least identifiable natural person are covered by the GDPR. According to the data protection authorities and case law, even email and IP addresses fall under PI.

Extraterritoriality

10 Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The GDPR generally applies the principle of territoriality, which limits the scope of the GDPR to its own jurisdiction and data controllers or processors established in the European Union or European Economic Area. Under certain conditions, the GDPR may also apply to data controllers outside the European Economic Area, if the data controller either:

- offers goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the European Economic Area; or
- monitors their behaviour as far as their behaviour takes place within the European Economic Area.

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

All processing or use of PI is covered by the GDPR as it follows a model in which every processing or every use of PI must be justified. Concerning data processing by a commissioned party on behalf of the data controller, some special regulations apply for the data controller as well as for the data processor. The responsibility for data controllers and data processors differs under the GDPR, even though data processors have broad responsibilities of their own.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Every collection, processing or use of PI must be justified under German data privacy law. This can either be done by the consent of the individual or by legal permission.

In practice, the following statutory legal permissions will be relevant:

- processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary for 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 that require protection of personal data, in particular where the data subject is a child (ie, the balance of interests).

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

Processing of sensitive personal data (eg, information on a person's racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life) is generally prohibited unless special conditions are met or the explicit consent of the data subject is obtained. Concerning data processing for business purposes, this is allowed when, for example:

- it is necessary for carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment and social security and social protection law;
- it 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;
- it relates to personal data that is manifestly made public by the data subject; or
- it is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Notice must be provided to every individual whose personal data the processor is processing. Information notices must at a minimum contain the following information:

- the data controller's identification;
- the data protection officer's contact details;
- the purposes of the processing;
- the legal basis for the processing;

- the legitimate interests, insofar as the data processing is based on article 6 (1) lit. f of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR);
- the recipients or categories of recipients; and
- the intention to transfer PI to a third country.

Additional information may be necessary, depending on the circumstances, to ensure lawful and proper processing. It is recommended that a more complete notice is provided to the affected data subjects since this will enhance trust in the processor's information practices.

If PI is not obtained directly from the individual (eg, marketing lists), then notice should be provided within a reasonable period, depending on the circumstances of the case.

Exemptions from transparency obligations

15 | When is notice not required?

Notice is not required if the individual is already acquainted with such information. Additional exemptions to the notice obligation are, for example:

- disclosure of PI would affect legal claims of the data controller; or
- PI was acquired from generally accessible sources and notification would require a disproportionate effort.

In addition to the above, there are a few more exemptions that either further legal obligations to keep data or the collection from publicly available data sources.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

As a general rule, appropriate steps must be taken to ensure correctness and accuracy for the purposes for which PI is obtained and processed.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

As a general rule, the amount of PI and the length of time it may be held are already limited by the applicable legal permission.

Beyond this basic restriction, data processing must be limited to what is necessary for the purposes of the processing. The principles of data minimisation, data avoidance and data economy apply.

This means that both the amount of data processed, the number of data subjects and the number of uses of the data must be reduced.

Three principles of data processing therefore apply:

- the data processing must be relevant to the purpose pursued (ie, it must be suitable to achieve a legitimate aim);
- the data processing must be necessary (ie, limited to what is necessary for the purpose pursued); and
- the data processing must be appropriate to the purpose, whereby an evaluative consideration must be conducted.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

As a general rule, the amount of PI and the length of time it may be held are already limited by the applicable legal permission.

Beyond this basic restriction, there is only an obligation to cease processing if the data subject lodges an objection with the controller and examination indicates that the legitimate interests of the data subject, owing to his or her particular personal situation, override the interests of the controller in such collection, processing or use or for the establishment, exercise or defence of legal claims, or in specific cases where PI is processed for advertising purposes.

Instead of ceasing, the GDPR normally demands the blocking of PI if the individual disputes its accuracy and its accuracy or inaccuracy cannot be verified.

The right to object to processing applies if interests worthy of protection based on a special personal situation outweigh the interests in the processing (this may apply to rare exceptions, such as a risk to life or limb (eg, risk of terrorism)) and in connection with any data processing for advertising purposes. When summarised, PI is legitimately intended to be disclosed to third parties, or to be processed on behalf of third parties without the consent of the individual for direct marketing purposes, if the data controller takes adequate measures to inform the individual about his or her right to object, the advertisement clearly identifies the body that first collected the data, and the transferring body records the source of the data and the recipient for two years following transfer and provides the individual with information about the source of the data and the recipient upon request.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI must be adequate, relevant and not excessive concerning the purposes for which it is processed.

PI must not be kept in a form that allows identification of the individual for longer than is necessary for the purposes for which it was collected or subsequently processed.

PI should not be subsequently or further processed in a way that is incompatible with the purposes for which it was obtained (principle of finality).

Further, the GDPR requires that data processing systems should be chosen and organised to collect, process and use as little PI as possible (principle of data minimisation). Specifically, the data should be rendered anonymous or given alias, as much as possible in light of the purpose for which it was collected or further processed and to the extent that the effort to do so is not disproportionate to the desired purpose.

The finality principle is adopted in German statutory data privacy regulations. As the purpose of any further data processing or use must be determined with collecting PI, every change of purpose needs a separate justification. General exemptions to this principle do not exist, but it is worth noting that data processing of special categories of PI follows special rules for justification in the GDPR.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

According to the GDPR, a decision based entirely on the fully automated processing of PI that produces a legal effect or significantly affects the data subject is generally prohibited. This prohibition covers such automated processing of PI that is in no way influenced by human intervention. Human intervention does not merely mean a formal intervention by a human being in the sense of a mere confirmation of the data processing, but requires human involvement of a substantive nature.

This does not apply to decisions that are based on one of the permissible elements of fundamental processing of PI and that are, additionally:

- necessary for the conclusion or performance of a contract;

- permitted by EU or member state legislation and such legislation contains appropriate measures to safeguard the rights and freedoms as well as the legitimate interests of the data subject; or
- conducted with the express consent of the data subject.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The data controller must implement appropriate technical and organisational measures to protect PI against loss or any form of unlawful processing (including theft, unlawful copying or recording). These measures must guarantee an appropriate level of security, consider the state of the art and the costs of implementation, and having regarded risks associated with the processing and nature of the data to be protected. Such measures should also aim to prevent the unnecessary collection and further processing of PI.

Regulation (EU) 2016/679 (the General Data Protection Regulation) provides for the following security measures, in particular, to be considered:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data promptly in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The data controller is further required to execute an information security agreement (a written data processor agreement) with service providers (regardless of the geographical location of such providers), which stipulates the technical and organisational measures to be considered. Additionally, the data controller is required to select only third-party service providers that offer adequate guarantees for technical and organisational information security.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Irrespective of the category of PI concerned, personal data breach notification is required if a breach of security occurs leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The data controller is exempt from notifying the relevant data protection authority (DPA) if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the individuals as well.

The data controller should notify the competent DPA and the individuals without delay. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Where notifying the individuals would require a disproportionate effect, such as in cases of very large numbers of persons concerned, a notification may be replaced by a public communication, or other means that would provide equivalent exposure given notifying the individuals.

Notification to the DPA must include a description of the nature of the personal data breach, contact details of the data protection officer (DPO), the proposed measures to limit possible negative consequences and the likely consequences of the unlawful disclosure.

Notification to the individuals concerned must at least include contact details of the DPO, the proposed measures to limit possible negative consequences and the likely consequences of the unlawful disclosure.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The controller is responsible for compliance with the principles for processing PI (lawfulness, fair processing, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality) and must also demonstrate compliance with them. This means that he or she must actively take measures to implement these principles. These measures must be reviewed, updated if necessary, adapted and replaced. In addition, the controller must document this and be able to provide evidence that the processing is carried out in accordance with the Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR). Neither the form nor the time limit of the proof is determined by law, so both are up to the decision of the controller. However, a register of processing activities must be kept by the controller and the processor (in the case of a company size of more than 250 employees or particular risks of data processing) in any case.

The DPA may request this evidence to verify the controller's compliance with the requirements of the GDPR. The burden of proof for compliance with the principles lies with the controller.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The appointment of a data protection officer (DPO) is mandatory if:

- the controller carries out automated processing with at least 20 employees;
- the core activities of the controller consist of processing operations that, by their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- the core activities of the controller consist of processing on a large scale of special categories of PI or PI relating to criminal convictions and offences; or
- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity.

The relevant data protection authority (DPA) must be notified of the DPO's engagement. The DPO is autonomous and is responsible for supervising data controllers' compliance with the GDPR. The DPO will maintain a register of processing operations and should possess adequate knowledge of the data controller's business, information practices and privacy legislation. Only persons with the specialised knowledge and reliability necessary to carry out their duties may be appointed. Further, there is broad dismissal protection for DPOs. Finally, they are legally entitled to participate in employer-sponsored education training.

DPOs can investigate the company's information practices and request information in the pursuit of their duties. The DPO should also handle the daily administration of privacy complaints and supervision and handle any prior checking, including for international transfers and sensitive data processing.

The DPO must meet the following criteria:

- the DPO must be a competent and reliable person who has the ability to perform the tasks specified in article 39 GDPR; and
- the DPO may not perform any other tasks that are incompatible with his or her supervisory function and could lead to conflicts of interest.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Individuals have a right to request detailed information about what data of theirs is processed and how it is processed. The data controller has to comply with all such requests every time. Therefore, data controllers are subject to various and partially very comprehensive data storage duties.

Automatic data processing also brings a general duty for documentation. Even if a DPO is appointed in the company, the data controller must still keep the necessary information at hand in this case for the DPA (details about the responsible data owner and the purpose of data processing, etc). Under the GDPR, the controller shall, in general, be responsible for, and be able to demonstrate compliance with, lawful processing (principle of accountability).

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

In principle, the data controller is obliged to comply with the provisions of the GDPR in full. However, the requirements for the data controller to comply must be proportionate. This means that the risks to the rights and freedoms of the data subjects must be objectively assessed. The type, scope, circumstance and purpose of the processing must be taken into account as risk factors. These must be evaluated taking into account the severity of possible (physical, material or immaterial) damage to the data subjects as well as the probability of occurrence. Lower damage can lead to an increased or high risk owing to a high probability of occurrence, whereas high damage can lead to a lower risk owing to a lower probability of occurrence. Consequently, this is a forecasting decision, the basis and decision of which must be documented.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The GDPR provides for specific obligations to establish data protection by design and to carry out data protection impact assessments. In particular, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, effectively and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR. The controller shall further implement appropriate technical and organisational measures for ensuring that, by default, only the PI that is necessary for each specific purpose of the processing is processed. Where a type of processing, in particular, using new technologies, and consider the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, before the processing, also assess the impact of the envisaged processing operations on the protection of personal data (data protection impact assessment).

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no general requirement to register with a data protection authority (DPA). The contact details of the data protection office, however, must be submitted to the DPA. The controller shall make its internal register of processing operations available to the DPA on request.

Other transparency duties

29 | Are there any other public transparency duties?

No such public transparency duties apply, except for the notification obligations in the case of personal data breaches.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Outsourced processing services will mostly be considered 'contract data processing on behalf' under Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR). Conditions apply to this kind of data processing.

There are minimum contents that a contract between the data controller and the processor must contain. For example, this contract must provide that the processor will:

- process the PI only on the documented instructions of the controller;
- ensure confidentiality and non-disclosure obligations;
- take technical and organisational measures to ensure the security of the processing;
- comply with the conditions for using other processors;
- assist the data controller in responding to requests;
- assist the data controller with other obligations, such as notification to the data protection authorities (DPAs);
- upon completion of the processing service, either delete or return all PI to the data controller; and
- provide the data controller with information and assistance to demonstrate compliance with its obligations and during audits.

However, this is only true for a processor that does not determine the purposes of processing by itself. If the controller transfers a whole function to the processor, which does not require the processor to follow instructions about how to process the data, the usual conditions for data transfers apply.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The term 'disclosure' is not defined in the GDPR but relates to making PI public and transferring PI from the data controller to a third party. Disclosure of personal data to another legal entity is permitted only if a

legal ground is presented and such disclosure is not incompatible with the purposes for which the PI was initially collected.

As the GDPR does not include an affiliated company privilege, every transfer of PI between two legally independent companies (including company group member entities) must be justified, meaning by law, consent or company agreement; this particularly applies if the receiving company has a registered office in a non-European Economic Area country.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Transfers outside the European Economic Area are only allowed to countries or territories that are considered by the European Commission to provide an adequate level of data protection. Transfers of personal data within the European Economic Area are not subject to such restrictions other than the requirement that a legal ground is presented and such disclosures not being incompatible with the purposes for which the PI was initially collected.

Transfers of PI outside the European Economic Area are only permitted if one of the exemptions listed in the GDPR applies or an adequate level of protection in the receiving country is available. Relevant exemptions for on-going data streams are still the new EU-approved data transfer agreements (Standard Contractual Clauses); and Binding Corporate Rules that are checked and formally confirmed by the responsible DPA, even though both instruments are under discussion following the Court of Justice of the European Union judgment invalidating the US Safe Harbor Agreement and the EU–US Privacy Shield (both of which were former instruments for data transfers from EU member states to the United States).

As there is not yet a successor agreement between the EU and the US regarding the transfer of data, such a transfer is currently legally very uncertain. In principle, the new standard contractual clauses can be concluded, but these alone are not sufficient. Further measures would have to be taken, but a legally secure data transfer is currently not possible, especially owing to the disclosure of data to US authorities. European companies must be advised to stop data transfers to the US, for example by seeking alternatives from service providers with servers in Europe.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Restrictions for data transfer in third countries apply to every form of data transfer, even if executed as contract data processing on behalf or as an onward transfer. Even the responsible entity outside Germany's jurisdiction must ensure that every service provider it assigns fulfils the requirements of German data privacy law.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no such requirement.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals have a right to request information from the controller on data relating to them, including the origin and recipients of the data, the purpose, recipients and retention periods (ie, right of access). The right of access implies that the data subject must be notified of all available data concerning the subject in the data file, including the available information on the source of the data. The controller shall provide a copy of the PI undergoing processing. Access must be provided in writing or the form of an email or fax, if appropriate in the given circumstances, without undue delay, free of charge and in any event within one month of receipt of the request. In practice, the right of access does not imply that a data subject can claim the right to obtain a copy of all documents included in a file (eg, a personnel file). Access does not need to be provided if, for instance:

- such is required to protect the overriding interests of third parties (eg, documents that contain personal information on other data subjects or that may be covered by an expectation of confidentiality);
- PI is stored due to a legal obligation or where used for purposes of data security or data protection control if providing the information would require an unreasonable effort; or
- PI is business-related and stored as required under the German tax and commercial laws, and is no longer needed for the original purposes, but retained due to a legal obligation.

Other rights

36 | Do individuals have other substantive rights?

Individuals have the following rights:

- to be informed (notice requirement);
- to request to rectify, supplement, delete or restrict PI relating to them that is inaccurate, incomplete or irrelevant for the processing, or is being processed in any other way that infringes a legal provision;
- to object to the processing of their PI if the processor bases the processing of PI on its proper legitimate interests (which do not outweigh the individual's privacy), which may be the case if the processor plans to provide PI to a third party or for processing of PI for marketing;
- to receive the PI concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format (data portability); and
- to be compensated if they suffer damage or distress as a result of a breach of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) or other data protection provisions.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Concerning unlawful data processing, the individual is granted a claim for damages against the responsible data owner by the GDPR. For serious breaches, the claim also covers injury to feelings; in all other cases, actual damage is required.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

A data protection authority (DPA) is only entitled to control the provisions of the GDPR and other data privacy regulations. It can punish the data controllers with administrative fines for this purpose. However, the DPA is not responsible for assigning damages claims against the data owners; these must be brought to the civil courts if necessary.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Alongside the limitations already shown above and the special limitations of area-specific rules, Regulation (EU) 2016/679 (the General Data Protection Regulation) provides some distinctive provisions for children's consent to the processing of special categories of PI, processing of PI relating to criminal convictions and processing that does not require identification.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The legal use of cookies is currently under discussion, because the relevant EU directive, Directive 2009/136/EC (the ePrivacy Directive) has not yet been implemented into German law, even though the transposition deadline has already expired. In the meantime, it remains unclear whether the use of cookies generally requires the consent of the individual and how this consent must be given (active opt-in as the safest option). It is therefore advisable to at least meet the recommendations the European Data Protection Board (EDPB), the former EU Article 29 Working Party, has issued about this matter. It is also recommended to use cookies primarily for statistical purposes and not for transferring user data to third parties. According to the recommendations of the EDPB, the various types of cookies should be distinguished. However, in all cases, the website's privacy policy should contain a description of how the PI is processed. Additionally, the cookie provider should grant the individual an opportunity to object against the use of the PI. On 24 May 2018, the German Data Protection Conference published a statement according to which tracking measures, including cookies, are only allowed after having obtained explicit consent. This means that informed consent within the meaning of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) must be obtained before data processing takes place, that is, before cookies are placed.

In October 2019, the Court of Justice of the European Union decided that the setting of cookies must be actively approved. A pre-set consent for saving the data is not permitted (judgment of 1 October 2019, case C-673/17). The user must be provided with clear and comprehensive information to easily determine the consequences of any consent he or she may give and to be able to give consent in full knowledge of the facts. The information must be clear and detailed enough to enable the user to understand how the cookies being used work. Those requirements derive from article 5 (3) of Directive 2002/58 (the ePrivacy Directive). Further, Directive 95/46 (the Data Protection Directive) provides additional information that must be provided. According to article 10 of the Data Protection Directive, this information includes, in addition to the identity of the controller and the purposes of the processing for which the data are intended, other information, for example, concerning the recipients or categories of recipients of the data, in so far as it is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

The ruling of the Court of Justice of the European Union has since been confirmed by the Federal Court of Justice in its judgment of 28 May 2020. The user's active consent to the collection and evaluation of data by cookies is required and a preselection may not be made in a cookie banner.

Since 1 December 2021, the new German Telecommunications-Telemedia Data Protection Act has been in effect, which now legally stipulates that the storage of information in the end user's terminal equipment or access to information already stored in the terminal equipment is only permitted if the end user has consented on the basis of clear and comprehensive information. Consent is only not required if the sole purpose of the storage or access is to carry out the transmission of a message over a public telecommunications network or if the storage or access is strictly necessary to enable the telemedia service provider to provide a telemedia service expressly requested by the user.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Prior consent is required to send commercial communications by electronic media (opt in as a general rule). Prior consent is, however, not required to send electronic communications to existing clients if the electronic contact details of the recipient were obtained by the sender in the context of the sale of its products or services. The sender may then use the electronic contact details for sending communication for commercial purposes if the message relates to the sender's own similar products or services and the recipient was offered the possibility to object (opt out). The recipient must be offered the opportunity to object to the use of its electronic contact details (in a free-of-charge and easy manner) at the moment of providing these details. If the recipient does not make use of the initial possibility to opt out at the time of the sale, the recipient should be offered the option to opt out in each subsequent transmitted communication. If such an objection is registered, the sender must take all steps to stop sending commercial messages by using electronic contact details.

No prior consent is required in respect of legal persons if the sender uses electronic contact details that were made public by the subscriber to be contacted. For instance, consent may be assumed if a legal person has made generally known that he or she wants to receive unsolicited marketing messages, has provided the email address where he or she wants to receive these messages and, if so desired, has indicated for what kind of messages this electronic contact may be used.

Further, no prior consent is required if the electronic message is sent to a subscriber located in a country outside the European Economic Area and the sender has fulfilled all provisions in that country concerning the sending of unsolicited communications.

Targeted advertising

42 | Are there any rules on targeted online advertising?

In principle, Recital 47 to the GDPR recognises data processing for the purpose of advertising in the online environment as a case of direct marketing as a legitimate interest, so the data processing can be based on the legal basis allowing processing for the purpose of safeguarding the legitimate interests of the data controller. Furthermore, the data processing could also be based on the consent of the data subject. The use of pseudonyms is likely to be required when creating usage profiles.

The use of online behavioural targeting may also be based on the legal basis of legitimate interest of the data controller, provided that the consent of the data subject has not been obtained. All circumstances of the individual case must be included in the necessary weighing of interests, such as the types of data used, the potential harassment of the advertising, the depth of intervention and the design of the information to be sent to the data subject in advance. In addition, any objections to this data processing by the data subject must be taken into account. Furthermore, the security measures taken are relevant for the balancing of interests, such as the use of pseudonyms or the separation of pseudonyms and clear names.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Processing of sensitive personal data (eg, information on a person's racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life) is generally prohibited unless special conditions are met or the explicit consent of the data subject is obtained. Concerning data processing for business purposes, this is allowed when, for example:

- it is necessary for carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment and social security and social protection law;
- it 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;
- it relates to personal data that is manifestly made public by the data subject; or
- it is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Profiling

44 | Are there any rules regarding individual profiling?

The GDPR distinguishes between 'automated decision-making in individual cases' and 'profiling'.

Not all profiling is also an automated individual decision. An automated individual decision is a decision based on automated processing that produces legal effects concerning the data subject or similarly significantly affects him or her. It does not necessarily require profiling, but can also be based on a different type of data processing. For profiling to be an automated individual case decision, other requirements must also be met.

In principle, the GDPR prohibits automated individual decisions. This is always the case if there is no human influence on the content of the decision. However, the GDPR also provides for exceptions to this.

Profiling is any type of automated processing of personal data that consists of using PI to evaluate certain personal aspects of a natural person. These can be, for example, aspects of work performance, health, economic situation, personal preferences and interests, reliability and behaviour, whereabouts and a change of location. These should be able to be analysed and predicted by means of profiling. The general rules of the GDPR apply to profiling, which means that the data subject can object to it and must be fully informed about the data processing.

The Working Party 29 has also published a working paper with guidelines on this, which have been endorsed by the EDPB.

HOFFMANN LIEBS

Peter Huppertz
peter.huppertz@hoffmannliebs.de

Kaiserswerther Straße 119
40474 Düsseldorf
Germany
Tel: +49 211 518 820
Fax: +49 211 5188 2100
www.hoffmannliebs.de

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Cloud computing services are services for commissioned data processing on behalf of the respective data controller. Hence, the data controller must meet all requirements for assigning data processors. Moreover, the data protection authorities have issued a guidance paper for using cloud computing services. According to this guidance paper, data controllers must implement sufficient control measures for the cloud provider, use data encryption where necessary, and safeguard that all requirements for cross-border transfers are met, if applicable. Essentially, this requires the data controller to:

- request transparent and detailed information from the cloud provider about its technical and organisational data security measures (safety concept), even for selecting the adequate cloud provider;
- provide for transparent, detailed and unambiguous contractual arrangements with the cloud provider, in particular concerning the location of data processing, notification about changes in the location, and portability and interoperability of the data in the case of, for example, the bankruptcy of the cloud provider;
- verify the implementation of the security measures that were agreed between the data controller and the cloud provider; and
- request current certificates from the cloud provider regarding the infrastructure the controller wants to use to safeguard information security, portability and interoperability of data.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Several data protection authorities (DPAs) have announced that they intend to concentrate more on sanctioning infringements shortly, so an increase in fines can be expected. Compared to the former legal situation in Germany, the number of reports, questions and complaints has risen sharply and has probably also led to relatively few fines being imposed to date because of the high burden on the authorities. Also, more complex facts lead to longer examinations and procedures under data protection law. However, the cases already prosecuted under Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) lead to the

conclusion that even in Germany there is an increasing tendency for companies, in particular, to face substantial fines if they fail to comply adequately with their obligations under the GDPR.

In 2020 and 2021, there was a sharp increase in fines. A total of over 1,000 fines were imposed since January 2020. The highest fine from 2020 in Germany was imposed on H&M. The textile trading company had to pay €35.2 million for the unlawful collection and storage of data concerning the private circumstances, including health data, of a large number of employees over many years. Another heavy fine (€10.4 million) was imposed on notebooksbiller.de for unlawful video surveillance of employees and customers over a period of at least two years.

In October 2021, the European Data Protection Board conducted a survey of European DPAs also regarding the number of data protection-related cases. This survey showed, among other things, that 43.31 per cent of the complaints by data subjects to the supervisory authorities in Germany had not yet been decided. However, with 40,309 complaint cases in 2020, Germany also has the most complaints. Germany is also far ahead in terms of data protection breach notifications, with 27,652 data protection breaches reported in 2020.

Hong Kong

Gabriela Kennedy and Joshua T K Woo

Mayer Brown

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Personal Data (Privacy) Ordinance (PDPO) (Cap 486) is the main legislation in Hong Kong that regulates the collection, use, transfer, processing and storage of PI.

The drafting of the PDPO was based upon:

- the International Covenant on Civil and Political Rights;
- the European Convention on the Protection of Human Rights and Fundamental Freedoms;
- the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; and
- EU Directive 95/46/EC.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Office of the Privacy Commissioner for Personal Data is the main body responsible for overseeing the enforcement of the PDPO and is headed by the Privacy Commissioner for Personal Data (PCPD).

The PCPD has various investigative powers, including the right to:

- undertake investigations and inquiries and issue enforcement notices in the event of any breach of the PDPO;
- enter any premises for investigation or inspection purposes (subject to certain requirements);
- conduct inspections on any PI system (ie, a system, whether or not automated, used in whole or in part, by a data user to collect, hold, process or use PI);
- summon and examine the claimant or any person who the PCPD believes has information regarding an investigation and require such persons to provide any information relevant to an investigation the PCPD is conducting;
- apply to court for permission to conduct search and seizure operations for evidence relating to certain doxxing offences;
- apply to court for an injunction relating to certain doxxing offences;
- directly prosecute certain doxxing offences, non-compliance with written notices issued by the PCPD and the obstruction of the PCPD's exercise of its statutory powers; and
- stop, search and arrest, without a warrant, an individual reasonably suspected to have committed doxxing offences that are directly prosecutable by the PCPD.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There is no legal obligation on the PCPD to cooperate with data protection authorities in other jurisdictions.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaching the PDPO may result in an inquiry, investigation and, for some doxxing-related offences, direct prosecution by the PCPD (either on the PCPD's own initiative or based on a complaint).

If a data user is found to have contravened any data protection principles in the PDPO, the PCPD may issue an enforcement notice requiring the data user to take steps to rectify the contravention. Failure to comply with such notice is a criminal offence, with the maximum penalty being a fine of HK$50,000 and two years' imprisonment (plus HK$1,000 daily if the offence continues). Repeated breaches of enforcement notices will result in higher fines of HK$100,000 and up to two years' imprisonment (plus HK$2,000 daily if the offence continues). Subsequent repeated contraventions of the PDPO on the same facts after an enforcement notice has been issued and complied with constitute an offence, and no new enforcement notice has to be issued. This attracts a HK$50,000 fine (plus HK$1,000 daily if the breach continues) and two years' imprisonment.

Contravening other requirements of the PDPO may also constitute an offence. Following the 2013 PDPO amendments, higher penalties have been introduced for breaches of the direct marketing provisions. Additional doxxing-related offences have been introduced following the 2021 PDPO amendments.

In particular, breaching the direct marketing requirements under the PDPO may attract a maximum fine of HK$500,000 and three years' imprisonment; whereas a breach involving the sale or transfer of PI to a third party for direct marketing purposes for the data user's gain may attract a maximum fine of HK$1 million and five years' imprisonment. Similarly, punishable by a fine of up to HK$1 million and five years' imprisonment is the disclosure of a data subject's PI:

- without the data subject's consent, with the intent to cause harm or recklessness about whether harm could be caused that results in harm caused; or
- obtained from a data user without the data user's consent, with the intent of personal gain or to cause loss to the data subject.

The maximum penalty for non-consensual disclosure of a data subject's PI with the intent to cause harm or recklessness about whether

harm could be caused (even if no actual harm is caused) is a fine of HK$100,000 and two years' imprisonment.

Following the 2021 PDPO amendments, the PCPD's investigation and enforcement powers for doxxing-related offences have been expanded; failure to comply with the PCPD's written or cessation notices, or obstruction of the lawful exercise of the PCPD's powers, are now directly prosecutable by the PCPD.

Failure to comply with the PCPD's written notices requiring the provision of assistance and materials, if done with fraudulent intent, may attract a maximum fine of HK$1 million and two years' imprisonment. Obstruction of the lawful exercise of the PCPD's powers is punishable by a maximum fine of HK$10,000 and six months' imprisonment, while failure to comply with a cessation notice may attract a maximum fine of HK$50,000 and two years' imprisonment (plus HK$1,000 daily while the offence continues). Subsequent failures to comply with cessation notices will result in a maximum fine of HK$100,000 and two years' imprisonment (plus HK$2,000 daily if the offence continues).

Other than criminal sanctions, data subjects aggrieved by contravention of the PDPO may seek compensation from the data user through civil action. The PCPD may assist data subjects in their civil action by providing legal advice or other assistance at its discretion.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Yes. Appeals against the PCPD's enforcement decisions may be made to the Administrative Appeals Board, which may confirm, amend or reverse the PCPD's decisions. Appeals against a cessation notice may also be made within 14 days of service, although the operation of the cessation notice will not be affected.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data (Privacy) Ordinance (PDPO) regulates both private and public sectors. However, some data users may be exempt from certain requirements under the PDPO, for instance, where PI is held or disclosed:

- for domestic or recreational purposes;
- by a court, magistrate or a judicial officer in the course of performing judicial functions;
- by or on behalf of the government to safeguard Hong Kong's security, defence or international relations;
- to prevent or detect crime; or
- solely for the purpose of news activity.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Electronic marketing activities are regulated by the PDPO if PI is used for 'direct marketing' purposes. Marketing through unsolicited electronic messages is regulated under the Unsolicited Electronic Messages Ordinance (UEMO) (Cap 593).

Interception of communications and surveillance conducted by or on behalf of law enforcement officers in Hong Kong is regulated under the Interception of Communications and Surveillance Ordinance (Cap 589) and the National Security Law (officially known as the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region).

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

The Office of the Privacy Commissioner for Personal Data (PCPD) has issued codes of practice, guidance notes and information leaflets that provide data protection guidance concerning specific industry sectors and activities, for instance, employee monitoring and the collection and use of PI through the Internet. Although these guidelines are not legally binding, the PCPD may take into consideration any non-compliance with these guidelines when determining whether a data user has contravened the data protection principles of the PDPO.

PI formats

9 | What categories and types of PI are covered by the law?

The PDPO covers PI in any form in which access to or processing of such data is practicable.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The PDPO does not have extraterritorial effect and only applies to data users who control the collection, holding, processing or use of PI in or from Hong Kong.

However, the Personal Data (Privacy) (Amendment) Ordinance 2021 has given the PCPD power to serve cessation notices on non-Hong Kong service providers if the PCPD has grounds to believe that there is an electronic doxxing message that the non-Hong Kong service provider is able to control, even if such an action is to be taken outside of Hong Kong.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The PDPO distinguishes between a 'data user' and 'data processor'. A data user is a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of PI; whereas a data processor is a person who processes PI on behalf of another person and does not process the data for any of its own purposes.

The PDPO only regulates data users but not data processors. As a consequence, if a data user engages a data processor to process PI on its behalf, it remains responsible in the event of any breach of the PDPO by its data processor.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes. A data user may collect PI from data subjects only if:

- the PI is collected for a lawful purpose directly related to a function or activity of the data user who is to use the PI;

- the collection of PI is necessary for and directly related to that purpose; and
- the PI is adequate, but not excessive concerning that purpose.

When collecting PI directly from a data subject, the data user is also subject to certain notification requirements, unless an exemption applies.

Also, consent is required if the PI will be used or transferred for direct marketing purposes, or for any other purpose that is not covered by the original collection purpose (as notified to the individual at the time of collection) or a directly related purpose unless an exemption applies.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

There is no concept of sensitive PI in the Personal Data (Privacy) Ordinance and there are no additional restrictions specifically imposed on sensitive PI. However, the Privacy Commissioner for Personal Data has published guidelines regarding the collection and use of certain PI that will require special attention. These include Hong Kong identity cards, biometric data and consumer credit data. These guidelines generally highlight the need for caution when handling these categories of PI and set out practical guidance on the proper collection and use of such PI.

In addition, there are certain industry-specific requirements imposed by the relevant regulators in respect of customer data held by regulated entities. For instance, the Hong Kong Monetary Authority has issued several circulars and guidelines relating to the protection and confidentiality of customer data that apply to all licensed banks regulated under the Banking Ordinance (Cap 155). Similar guidelines have also been issued by regulators in other sectors of the financial industry such as the Insurance Authority and the Securities and Futures Commission.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Yes. Notification obligations apply where PI is collected directly from a data subject. On or before the collection of PI from a data subject, the data user must:

- inform the data subject as to whether the data subject is obligated to supply the PI and, if the data subject is obligated to supply it, the consequences of him or her failing to supply the PI;
- inform the data subject on or before collecting the PI as to the purpose for collecting the PI and the classes of persons to whom the data may be transferred; and
- inform the data subject of his or her right to request and receive access to the PI collected, and the name or job title and address of the individual who is to handle any such data access or correction request.

Additional notification requirements will apply if the PI will be used for direct marketing purposes.

Exemptions from transparency obligations

15 | When is notice not required?

Notice is not required if the PI was not collected directly from the data subject or the data was anonymised and it is not possible to reidentify the data subject (since such data will not constitute PI under the Personal Data (Privacy) Ordinance (PDPO)).

Where PI is collected directly from the data subject for certain stipulated purposes, notice is also not required if the provision of such notice would likely prejudice these purposes. These exempted purposes include:

- identifying an individual who is reasonably suspected to be, or is, involved in a life-threatening situation;
- emergency relief;
- prevention or detection of crime;
- apprehension or collection of any tax or duty;
- prevention or remedying of unlawful or seriously improper conduct or dishonesty by persons; and
- ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on anything to which the discharge of statutory functions by the data user relates.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

The PDPO requires data users to take all practicable steps to ensure that PI is accurate regarding the purpose for which it is to be used. Data subjects also have the right to request correction of their PI held by a data user. If PI is found to be inaccurate, data users should either rectify or erase the data.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

No, as long as the threshold requirements for data collection are fulfilled. A data user may collect PI only:

- for a lawful purpose directly related to a function or activity of the data user who is to use the PI;
- if the collection is necessary for and directly related to that purpose; and
- if the PI is adequate but not excessive concerning that purpose.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Under the PDPO, data users must take all practicable steps to ensure that PI is not held longer than is necessary to fulfil the purpose (or a directly related purpose) for collection and is erased when it is no longer required for such purposes, unless any such erasure is prohibited by law or its retention is in the public interest (eg, historical interest).

In addition, where data users engage data processors, they must adopt contractual or other means to prevent their data processors from keeping PI longer than is necessary for processing the data.

While the PDPO does not stipulate any retention periods for PI, data users should refer to the requirements under other statutes and guidelines issued by the PCPD and other industry-specific regulators. For instance, the PCPD's Code of Practice on Human Resource Management provides that employers may retain an employee's PI for up to seven years after the end of his or her employment, unless there is an existing reason requiring the employer to hold the data for a longer

period or the data is necessary for the employer to comply with contractual or legal obligations.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes. PI may not be used for any purpose other than the data user's stated purpose (or a directly related purpose) for which the PI was to be used at the time of collection, unless the data subject's express consent is obtained.

Any use of PI for new purposes requires the prescribed consent of the data subject concerned.

There are certain exceptions to the consent requirement. These exceptions include:

- where the PI will be used for one of the following purposes and obtaining consent will likely prejudice such purpose:
  - the prevention or detection of a crime;
  - the apprehension, prosecution or detention of offenders;
  - the assessment or collection of any tax or duty;
  - the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, dishonesty or malpractice by individuals;
  - the prevention or preclusion of significant financial loss arising from imprudent business practices or activities of persons, or the unlawful or seriously improper conduct, dishonesty or malpractice by persons; or
  - the determination of whether the data subject's character or activities are likely to have a significantly adverse impact on anything to which the discharge of statutory functions by the data user relates;
- where the PI relates to a data subject's identity, physical or mental health or location and obtaining consent would likely cause serious harm to the data subject's physical or mental health or that of another individual;
- where the PI is required in connection with any legal proceedings in Hong Kong or to establish, exercise or defend any legal rights in Hong Kong; or
- where the PI will be transferred or disclosed by a data user for due diligence relating to a business transaction for the transfer of the business or property of or shares in the data user, or an amalgamation of the data user with another body; this is subject to the primary purpose of the proposed business transaction not being the transfer, disclosure or provision of PI for gain, as well as other requirements imposed by the PDPO.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

No. However, the PCPD published a Guidance Note on the Ethical Development and Use of AI in August 2021 setting out considerations that data users should contemplate when using AI and PI, including:

- the permissible uses of the PI used to train AI models (training data), and whether such use would comport with the original purpose for its collection and use (Data Collection Principle (DPP) 3);
- the volume of the training data required is not excessive (DPP 1);
- the sensitivity of the PI involved and whether it is necessary for the intended purposes (DPP 1);
- the quality of the data involved (eg, its accuracy) (DPP 2);
- the security of the PI when used to develop or used by the AI (DPP 4); and
- the probability of privacy risks arising and the potential harm that may result.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Under the Personal Data (Privacy) Ordinance (PDPO), data users are required to take all practicable steps to ensure that PI is safeguarded against unauthorised or accidental access, processing, erasure, loss or use. In addition, where data processors are engaged (in or outside of Hong Kong), data users are required to adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data they transferred to their data processors.

The PDPO does not stipulate any mandatory security measures to be implemented by data users. Data users must have regard to the following factors in determining what constitutes 'practical steps' on a case-by-case basis:

- the nature of PI and the harm that could result in the event of any unauthorised or accidental access, processing, erasure, loss or use of the PI;
- the physical location where the PI is stored;
- any security measures used in the equipment storing the PI;
- any measures taken to ensure the integrity, discretion and competence of people who are authorised to access the PI; and
- any measures taken to ensure that the PI are safely transmitted.

Additional industry-specific requirements relating to the protection of customer data have been imposed on financial institutions through various circulars and guidelines issued by the relevant regulators. For example, the Outsourcing module (SA–2) of the Supervisory Policy Manual issued by the Hong Kong Monetary Authority requires all authorised institutions to implement proper controls for the protection of customer data when entering into an outsourcing arrangement. These controls include:

- undertakings by the service provider that the company and its staff will abide by confidentiality rules and the data protection principles under the PDPO;
- ensuring the authorised institution has contractual rights to take action against the service provider in the event of a data breach;
- segregation or compartmentalisation of the authorised institution's customer data from the data of the service provider and its other client; and
- ensuring that access rights to the authorised institution's data are only delegated to authorised employees of the service provider on a need basis.

The Insurance Authority has also issued a Guideline on Cybersecurity that requires authorised insurers to implement robust cybersecurity frameworks to protect the PI of their existing or potential policyholders. Such cybersecurity frameworks should be tailored to the nature, size and complexity of the insurer's business and include certain measures, such as:

- ensuring proper governance (eg, the board of directors of the insurer should have overall responsibility and ensure accountability for cybersecurity controls);
- identifying cyber risks and regularly assessing the effectiveness of the risk control measures;

- implementing continuous monitoring processes for early detection of cybersecurity incidents;
- developing a cybersecurity incident response plan; and
- establishing cyber risk information sharing processes and providing adequate training for all system users.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

While there is no statutory requirement to do so, voluntary notification is generally recommended by the Privacy Commissioner for Personal Data. Industry-specific regulators may also require companies in such regulated industries (eg, financial institutions) to notify individuals of any unauthorised access, use or loss of their PI. Under the Guidance Note on Data Breach Handling, the PCPD defines data breaches as suspected breaches of data security of PI held by the data user that exposes the PI to the risk of unauthorised or accidental access, processing, erasure, loss or use.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

There are no requirements for data users to implement internal controls, although doing so would allow the data user to better comply with its obligations under the Personal Data (Privacy) Ordinance (PDPO) (eg, complying with Data Collection Principle 2(2) to ensure that it has taken all practicable steps to ensure that PI is not retained longer than necessary for the fulfilment of the purpose for which the data is to be used).

Internal audit and assurance programmes to monitor compliance with PI protection policies are recommended in the Privacy Commissioner for Personal Data's (PCPD) Privacy Management Best Practice Guide issued in February 2014.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The Personal Data (Privacy) Ordinance (PDPO) does not require data users to appoint a data protection officer. However, the Privacy Commissioner for Personal Data (PCPD) issued a best practice guide on a privacy management programme that recommends that organisations appoint a data protection officer who is responsible for overseeing the organisation's compliance with the PDPO.

The responsibilities of a data protection officer typically include the following:

- setting up and implementing programme controls of the privacy management programme in the organisation;
- coordinating with other persons responsible for related disciplines and functions within the organisation;
- assessing and revising the said programme controls on an ongoing basis;
- representing the organisation in the event of an enquiry, inspection or investigation by the PCPD; and
- advocating PI protection within the organisation.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Data users must keep a logbook to record each data access request and data correction request received and that have been refused, including the reasons for the refusal. Each log entry should be retained for at least four years from the date the entry was made.

Apart from the above, there are no other legal requirements to maintain any internal records or establish internal processes or documentation for data users or processors.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

No, but the PCPD has issued a leaflet advising data users to adopt privacy impact assessments before launching any new business initiatives or projects that may have a significant impact on personal data privacy.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The PDPO does not specifically impose obligations concerning PI processing systems.

However, the PCPD has released several guidance notes and information booklets that recommend data users to apply a privacy-by-design approach and carry out privacy impact assessments when undertaking new business projects or processing operations that involve the collection of a large volume of data or the use of more intrusive and new technologies in the collection of data.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no legal requirement for a data user or data processor to register with the regulatory authority. However, part 4 of the Personal Data (Privacy) Ordinance (PDPO) has in place a data user return scheme that enables the Office of the Privacy Commissioner for Personal Data (PCPD) to require certain categories of data users to periodically provide returns to the PCPD setting out prescribed information, (eg, the type of PI held, the purposes of collection, etc). No such categories of data users have ever been specified and part 4 of the PDPO is not in effect.

Other transparency duties

29 | Are there any other public transparency duties?

The PDPO requires a data user to be transparent about their data collection and take all practicable steps to disclose their privacy policies and practices to the public, including information as to the types of PI held by them and the main purposes for which the PI will be used.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

A data user may transfer PI to a third-party service provider to process data on its behalf, provided such transfer and purposes have been notified to the data subject at the time of collection. Otherwise, consent is required if the PI will be transferred for any other purpose that is not covered by the original collection purpose or a directly related purpose unless an exemption applies.

In addition, the data user must adopt contractual or other means to prevent:

- PI that is transferred to the data processor from being kept for longer than is necessary for the processing of such PI; and
- any unauthorised or accidental access, processing, deletion, loss or use of the PI that is transferred to the data processor.

In September 2012, the Office of the Privacy Commissioner for Personal Data (PCPD) also issued guidelines on Outsourcing the Processing of Personal Data to Data Processors. While the guidelines are non-mandatory, failure to comply may be taken into account by the PCPD when assessing whether a breach of the Personal Data (Privacy) Ordinance (PDPO) has occurred.

These guidelines include recommendations on the provisions that should be included in the agreement between a data user and a data processor. For example, the agreement should:

- require the data processor to notify the data user in the event of any suspected unauthorised disclosure, use or loss of the PI;
- prohibit the data processor from using the PI for any purpose other than the purpose for which it was provided; and
- specify the security measures that the data processor must implement to protect the PI.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Apart from the requirements relating to the transfer of PI to data processors, the transfer of PI for direct marketing purposes and the transfer of PI outside Hong Kong, there are no specific restrictions on the disclosure of PI to other recipients.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Currently, there are no restrictions in effect concerning the cross-border transfer of PI apart from general notification and consent requirements as described and any provisions concerning transferring PI to a third party for direct marketing purposes.

While section 33 of the PDPO provides for restrictions for cross-border transfers of PI, this section remains the only section of the PDPO yet to come into effect. No timetable has been announced for its implementation. However, the PCPD has issued a non-binding guidance note on cross-border data transfers, which recommends that data users comply with section 33 even before its implementation. If section 33 is implemented, data users may only transfer PI from Hong Kong to other countries under specified circumstances, for instance, where the data subject has consented to the transfer in writing, the recipient jurisdiction is included in a 'white list' issued by the PCPD, or the data user has taken all reasonable precaution and exercised due diligence in ensuring that the data transferred will not be used in a manner in violation of the PDPO.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Currently, there are no restrictions in effect concerning the cross-border transfer of PI apart from the general notification and consent requirements and any provisions concerning transferring PI to a third party for direct marketing purposes.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no such localisation restrictions under Hong Kong law.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes. A data subject may request to be informed if a data user collects information about them. If the data user has collected PI relating to the data subject and the data subject requests access to such data, the data user must comply subject to certain exceptions.

A written request from a data subject asking to access or receive a copy of his or her PI held by the data user must be complied with within 40 calendar days from the date of receipt of the request. If a data access request cannot be complied with within the 40-day deadline, then the requestor must be informed of this before the expiry of that deadline and must be provided with a copy of the requested PI as soon as practicable.

Even if the data user does not hold any PI of (or the PI specifically requested by) the data subject, it must notify the requestor of this fact within 40 calendar days from the date it received the request.

A data user can only refuse to comply with a data access request if one of the exemptions below applies:

- if the PI will be used for the following purposes, and granting a data access request to the data subject will prejudice such purposes, or directly or indirectly identify the person who is the source of the data:
  - the prevention or detection of crime;
  - the apprehension, prosecution or detention of offenders;
  - the assessment or collection of any tax or duty;
  - the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;
  - the prevention or preclusion of significant financial loss arising from any imprudent business practices or activities of persons or the unlawful or seriously improper conduct, or dishonesty or malpractice, by persons; and
  - ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on anything to which the discharge of statutory functions by the data user relates;
- the PI requested consists of information relating to the data user's staff planning proposal regarding hiring or redundancy proposals;

- the PI requested forms part of an evaluative process (eg, consideration for recruitment, promotion, discipline or dismissal of an employee, or in connection with the awarding of any benefits or bonuses) before the relevant decision has been made;
- the PI requested is a personal reference provided by another individual (unless that other individual has consented to the disclosure or the requesting party has already been informed in writing that he or she has been accepted or rejected to fill the relevant position);
- the PI requested is held by or on behalf of the Hong Kong government, to safeguard the security, defence or international relations in respect of Hong Kong;
- the PIrelates to the physical health, mental health, identity or location of a data subject, and granting the request would likely cause serious harm to the physical or mental health of the data subject or any other individual;
- the PI consists of information that is subject to legal professional privilege;
- if compliance with the data access request will result in the data user being incriminated in any proceedings for an offence, other than an offence and the Personal Data (Privacy) Ordinance (PDPO);
- the data access request is not made in writing;
- the data access request is not made in the English or Chinese language;
- insufficient information has been provided to enable the data user to locate the PI;
- if the identity of the requestor is in doubt, and the data user cannot reasonably ascertain their identity;
- the PI requested is not held by the data user;
- copy of the requestor's PI cannot be provided without disclosing the PI of another individual unless that individual has consented to the disclosure of their data to the requestor, or the PI relating to the other individual can be redacted or removed; or
- the PI is otherwise exempted from disclosure under the PDPO.

If the data user rejects or denies a data access request (as permitted under the PDPO), then it must inform the requestor within 40 calendar days from the date it received the request and explain why it cannot comply with his or her request. When a copy of the requestor's PI is provided, any PI relating to a third party should not be included or should be redacted.

Other rights

36 | Do individuals have other substantive rights?

There is no express right under the PDPO for individuals to request the deletion of their PI. However, individuals have the right to request the correction of their PI held by a data user. In addition, individuals have the right to request that data users cease using their PI for certain purposes (eg, direct marketing purposes).

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under section 66 of the PDPO, individuals have the express right to seek compensation from a data user for any damage (including injury to feelings) suffered as a result of any breach of the PDPO by the data user. In addition, legal assistance can be granted to such individuals at the Privacy Commissioner for Personal Data's (PCPD) discretion.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

If a data user fails to comply with a data access or correction request in breach of the PDPO, the data subject may file a complaint with the PCPD. If the PCPD is satisfied that there is a contravention of the PDPO after conducting an investigation, he or she may serve an enforcement notice on the data user requiring the data user to take steps to rectify the contravention. In addition, the data subject may claim compensation against the data user for contravening the PDPO through civil proceedings if the data subject had suffered any harm.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

There are no additional exclusions or limitations apart from those already described.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Cookies are governed by the Personal Data (Privacy) Ordinance (PDPO) to the extent that they amount to PI. If it is reasonably practicable to ascertain an individual's identity directly or indirectly from the cookies (either individually, combined or with other data), such collection will likely fall within the scope of the PDPO.

In addition, the Office of the Privacy Commissioner for Personal Data (PCPD) has issued an information leaflet on online behavioural tracking, which provides several recommended practices for data users concerning the use of cookies or online behavioural tracking mechanisms on their websites. Data users are advised to:

- inform website users of, among other things, the types of information being collected or tracked, the purpose of collection, and whether their behavioural information is collected or tracked by any third parties via the website;
- inform website users of the means of disabling the cookie or tracking mechanism, or alternatively, if website users are not permitted to do so, justify the reasons;
- pre-set a reasonable expiry date for cookies;
- encrypt the contents of cookies where appropriate; and
- avoid using techniques that disregard browser settings on cookies, unless an option is provided to website users to reject or disable such cookies.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

There are stringent requirements under the PDPO on the use of PI in direct marketing. Direct marketing means 'the offering, or advertising of the availability, of goods, facilities or services or the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes through direct marketing means', such as sending information or goods, addressed to a specific person by name, mail, fax, email or other forms of communication (eg, social media).

Concerning direct marketing, data users are required to:

- inform the data subject of the type of goods, facilities or services that will be marketed and the specific type of PI that will be collected and used for direct marketing purposes (eg, name and email address, etc);
- if the data user will transfer the PI to a third party for their use in direct marketing, the data user must notify the data subject, in writing beforehand of:
  - its intention to transfer the data to a third party for direct marketing purposes, and that it cannot do so without the data subject's consent;
  - the classes of transferees;
  - the categories of goods or services that may be marketed by the transferees; and
  - whether or not the data user is transferring it in return for gain; and
- obtain the prescribed consent of the data subject for such use and transfer.

The data subject must have explicitly indicated that he or she does not object to the use or transfer of his or her PI to a third party for the purposes of direct marketing. Therefore, data users can obtain valid consent by either using an 'opt-in' or 'opt-out' method.

In addition, when a data user uses an individual's PI for the first time for direct marketing purposes, the individual must be informed of his or her right to withdraw his or her consent at any time.

The PDPO generally distinguishes between a breach of the direct marketing requirements involving the sale or transfer of PI to a third party for gain, and a breach of the direct marketing requirements otherwise than for gain. A breach of the former may attract a maximum fine of HK$1 million and five years' imprisonment; whereas a breach of the latter may attract a maximum fine of HK$500,000 and three years' imprisonment.

However, the PCPD has indicated that he or she will not enforce the direct marketing requirements for any direct marketing conducted in a purely business-to-business context. The PCPD will consider the following factors when determining whether the business-to-business exception will apply:

- the circumstances under which the PI is collected, for example, whether the PI concerned is collected in the individual's official capacity;
- the nature of the products or services, that is, whether they are for the use of the corporation or personal use; and
- whether the marketing effort is targeted at the corporation or the individual, where the products or services can cater for either use of the corporation or personal use.

The PCPD has been actively monitoring and enforcing the direct marketing requirements in the PDPO. In 2019 alone, there were multiple cases where the data user was fined for breaching the direct marketing requirements and the largest fine imposed that year was HK$84,000 in total (HK$6,000 per charge against the relevant data user), which was the second-highest quantum of fine imposed since the amendments to the direct marketing provisions in the PDPO took effect in 2013.

Separately, the Unsolicited Electronic Messages Ordinance (UEMO) regulates the sending of commercial electronic messages (including pre-recorded telephone messages, faxes, text messages and emails) for offering, supplying or promoting goods, services, facilities, land or business opportunities, among other things.

Individuals can register their telephone and fax numbers on a 'do-not-call' register to stop unsolicited commercial electronic messages from being sent to them. Any party that sends an unsolicited commercial electronic message to a number that is registered on the do-not-call register will be in breach of the UEMO.

Organisations can send unsolicited commercial electronic messages to any telephone or fax number that is not registered on the do-not-call register, subject to their compliance with the UEMO and related regulations. For example, a sender must:

- display its number when sending messages;
- clearly identify itself and provide contact information in the message; and
- offer recipients a way to unsubscribe.

Targeted advertising

42 | Are there any rules on targeted online advertising?

No. However, the PCPD has issued an information leaflet on online behavioural tracking setting out recommendations on the use of cookies and factors that data users should consider when deploying online tracking tools.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

No. However, the PCPD has issued guidelines highlighting the need for caution when handling certain sensitive categories of PI (such as Hong Kong identity cards, biometric data and consumer credit data) and setting out practical guidance on the proper collection and use of such data.

Profiling

44 | Are there any rules regarding individual profiling?

No. However, the PCPD has issued an information leaflet on online behavioural tracking that recommends practices on transparency concerning profiling users, as well as guidelines on AI regarding the use of automated systems for profiling.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

While the PDPO does not provide for specific rules on the use of cloud computing services, the PCPD has issued an information leaflet on cloud computing that provides several recommendations for data users in using cloud computing services. For instance, data users are recommended to:

- inform data subjects of the locations where the cloud services provider would store their PI;
- inform data subjects of any cross-border transfer of their PI in using the cloud services;
- select a cloud services provider that allows them to specify locations where there is an adequate level of privacy protection to PI;
- verify the data protection commitments by the cloud services provider; and
- ascertain whether the cloud services provider engages in sub-contracting arrangements, and if so, obtain formal assurance that any sub-contracting will be under the same level of protection as applicable to the said provider.

The PCPD also noted that data users generally retain a lower level of control over PI stored on the cloud when using the 'software as a service' model of cloud computing (as opposed to the 'infrastructure as a service' or 'platform as a service' models) and shared public clouds

(as opposed to private clouds). In such circumstances, data users should carefully review the risks associated with such arrangements and seek ways to manage them.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Personal Data (Privacy) (Amendment) Ordinance 2021 (the Amendment Ordinance) became effective on 8 October 2021 to combat doxxing (ie, unauthorised disclosure of one's PI as a means of harassment) in Hong Kong more effectively.

The Privacy Commissioner for Personal Data (PCPD) has encountered numerous obstacles in its efforts to curb doxxing activities since 2019, given its lack of power to compel online platforms (acting as data processors) to remove doxxing posts.

With the passage of the Amendment Ordinance, doxxing is addressed by:

- criminalising doxxing acts under two new direct offences;
- empowering the PCPD to carry out criminal investigations and prosecution of some offences under the Personal Data (Privacy) Ordinance (including doxxing-related offences); and
- conferring on the PCPD statutory powers to serve cessation notices to demand actions cease or to restrict disclosure of doxxing content.

Since the Amendment Ordinance became effective, the PCPD has made two arrests for suspected doxxing offences.

MAYER | BROWN

Gabriela Kennedy
gabriela.kennedy@mayerbrown.com

Joshua T K Woo
joshua.woo@mayerbrown.com

16th–19th Floors
Prince's Building
10 Chater Road
Central
Hong Kong
Tel +852 2843 2211
www.mayerbrown.com

Hungary

Endre Várady, János Tamás Varga and Andrea Belényi

VJT & Partners

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The general Hungarian regulatory instruments for the protection of PI are the EU General Data Protection Regulation (GDPR) and Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Data Protection Act).

The Data Protection Act was amended in July 2018 to implement the GDPR in Hungary. The Data Protection Act contains provisions spanning three categories:

- provisions applying to data processing that are under the scope of the GDPR. These are additional procedural and substantial rules, where the GDPR permits derogation or the application of national laws;
- provisions applying to data processing operations that fall outside the scope of the GDPR; and
- provisions applying to data processing for law enforcement, national security and national defence purposes to implement Directive (EU) 2016/680 (the Law Enforcement Directive).

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The authority responsible for overseeing the data protection law is the National Authority for Data Protection and Freedom of Information (the Authority). The Authority has the following investigative powers:

- it may ask for information and request the client to make statements;
- it may take testimony from witnesses (including conducting interviews);
- it may access all PI and information that is necessary for the performance of its tasks;
- it may also ask for copies of PI and other information;
- it may make on-site visits and request access to equipment used in the course of the data processing; and
- it may ask for expert opinions.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Authority is a member of the European Data Protection Board (EDPB) that publishes guidelines to ensure consistency across member states in GDPR interpretation. Regarding issues that are covered by guidelines of the EDPB or the article 29 of the Data Protection Working Party (the predecessor of the EDPB), the Authority follows those guidelines.

In the case of cross-border data processing, the Authority suspends the proceeding until the lead supervisory authority makes its statements on taking over the case based on the GDPR's one-stop shop. In such cases, the lead supervisory authority and the Authority must cooperate to find a mutually acceptable solution. If they cannot, the consistency mechanism applies, in which the EDPB may have the final word.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches may lead to sanctions, which depend on the type of breach. The most feared sanction is the administrative fine for breaching the GDPR, which may reach €20 million or 4 per cent of the organisation's annual turnover (whichever is higher).

The Authority may also impose corrective measures set out under the GDPR such as:

- issuing reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR;
- ordering the controller or the processor to comply with the data subject's request to exercise his or her rights;
- ordering the controller or processor to make their processing operations comply with the provisions of the GDPR;
- ordering the controller to communicate a personal data breach to the data subject;
- imposing a temporary or definitive limitation (a ban on processing);
- ordering the rectification or erasure of PI or restriction of processing;
- ordering the suspension of data flows to a recipient in a third country or an international organisation; and
- withdrawing a certification or ordering the certification body to withdraw a certification.

A breach of data protection laws may also lead to criminal penalties if such a breach is committed for financial gain or if it causes significant detriment for individuals. The Authority has two kinds of procedures to handle breaches:

- Investigation: the Authority may start an investigation based on a complaint (which may be made by anyone) or ex officio. At the end of the investigation, the Authority may impose an order to remedy the situation. The controller shall remedy the situation within 30 days of receiving the order. In the investigation procedure, the Authority neither imposes a fine nor other corrective measures.
- Administrative procedure: the administrative procedure may be launched based on a complaint (only the concerned data subject may make a complaint) or ex officio. The Authority will launch the administrative procedure ex officio only if in the investigation phase the Authority had imposed an order, but the controller did not remedy the situation within the deadline, or in the investigation phase, the Authority concluded that unlawful processing occurred and based on GDPR rules a fine may be imposed.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Yes, the PI owners may appeal to the Budapest Regional Capital Court against orders of the Authority.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Hungarian data protection laws cover all types of organisations. An exemption applies in the case of individuals processing PI for household purposes, but otherwise, any organisation that processes PI will be under the scope of Hungarian data protection laws.

Even when the EU General Data Protection Regulation (GDPR) does not apply (eg, the processing of PI by national security entities or courts), the provisions of Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Data Protection Act) still apply. In such a case, the National Authority for Data Protection and Freedom of Information (the Authority) will remain the supervisory authority with a limited corrective power to impose a fine of up to 20 million forints. In the case of PI processing by the courts, the processing will be supervised by the courts (not the Authority).

As these exemptions are rare, this chapter focuses only on the processes that fall under the scope of the GDPR.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The GDPR and the Data Protection Act cover these areas together with specific Hungarian national legislation such as:

- communications interception: Act XC of 2017 on Criminal Procedure and Act C of 2003 on Electronic Communications;
- electronic marketing: Act XLVIII of 2008 on Commercial Advertisement and Act CVIII of 2001 on Electronic Commerce; and
- the monitoring and surveillance of individuals: Act CXXXIII of 2005 on Private Security and the Activities of Private Investigators, and numerous other acts depending on which locale the surveillance of individuals takes place (eg, in streets, stadia or vehicles).

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Apart from the general data protection framework, there is separate legislation for sector-based data protection rules, including in areas such as marketing, the financial sector, e-commerce, employment, healthcare and CCTV. In April 2019, the Hungarian parliament adopted a new GDPR implementation package amending 86 sector-based laws.

PI formats

9 | What categories and types of PI are covered by the law?

The Hungarian lawmaker extended the material scope of the GDPR. The Hungarian data protection law covers all forms of PI, not just electronic records, but also manual data processing and – unlike other countries – even when the PI does not form part of a filing system.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Hungarian data protection laws also apply to PI controllers and processors established or operating outside of Hungary if:

- the controller's main establishment is located in Hungary, or the controller's only place of business within the European Union is in Hungary; or
- the controller's main establishment is not located in Hungary or the controller's only place of business within the European Union is not in Hungary, but the controller's or its processor's data processing operation relate to:
  - the offering of goods or services to data subjects located in Hungary, irrespective of whether a payment of the data subject is required; or
  - the monitoring of data subjects' behaviour that occurs in Hungary.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

All processing (except processing by individuals for household purposes) and all operations on the PI (eg, collection, storage and disclosure) are covered by Hungarian data protection laws.

A distinction is made between the controller who determines the purpose and the means of the data processing and the processor who merely executes the decisions of the controller and processes the PI on behalf of the controller. The processor is not entitled to make any decision on the merits of the data processing.

The controller is primarily responsible for the lawfulness of data processing. However, some obligations directly apply to processors (eg, taking appropriate data security measures) and they may be directly liable if they breached such obligations.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

There must be a specific ground on which the controller may hold PI. Six legal grounds exist:

- the data subject's consent;
- the necessity for the performance of a contract (to which the data subject is party or to take steps at the request of the data subject before entering into a contract);
- the necessity for compliance with a legal obligation to which the controller is subject (Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Data Protection Act)) adds that such legal obligation must be set out in an act of the parliament or a municipal decree);
- the necessity to protect the vital interests of the data subject or another natural person;
- the necessity for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; and
- the necessity for the legitimate interests of the controller or by a third party.

The National Authority for Data Protection and Freedom of Information argues that, in the case of holding special categories of PI, apart from having one of the six legal grounds above, the controller must also check whether one of the conditions of article 9 of the EU General Data Protection Regulation applies (eg, the data subject needs to give explicit consent or the processing needs to be necessary to exercise or defend legal claims).

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Apart from the general rules for holding sensitive PI, Hungarian law restricts the processing of certain sensitive PI. The most relevant restrictions include:

- health data may be processed only based on the consent of the data subject or if the controller is authorised to process the data based on the authorisation of Act XLVII of 1997 on the processing of health data and for the purposes defined in the Act;
- employees' biometric data may be processed for identification purposes under limited conditions (eg, unauthorised access would lead to a threat to life or health); and
- employees' or job applicants' criminal data may be processed for vetting purposes only if the applicable Hungarian legislation authorises it, or if it is necessary to protect the employer's significant financial interests, to protect secret information (set by law), or to protect some other specific legitimate interests of the employer (eg, firearms' storage or chemical materials).

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The EU General Data Protection Regulation (GDPR) applies directly. Controllers must notify data subjects whose PI they hold. The notice must contain the elements of article 13 of the GDPR (if PI is obtained from data subjects) or article 14 of the GDPR (if PI is not obtained from data subjects).

The National Authority for Data Protection and Freedom of Information (the Authority) takes a granular approach as it requires detailed notice about the elements of article 13 or 14 of the GPDR on the purpose level. This means that the controller must first define the purpose and then all the relevant information for each data processing purpose must be provided.

The Authority states that the purpose needs to be as specific as possible (eg, 'marketing' is incorrect, as it allows different interpretations, 'sending newsletters' is correct as it allows only one interpretation). If the data was collected for one purpose, in principle, it should not be used for another purpose.

As a general rule, the notice must be provided at the time the PI is collected from the data subject or (if the PI is not directly collected from the data subject) within a maximum of one month after obtaining the PI.

Exemptions from transparency obligations

15 | When is notice not required?

It is not necessary to notify the data subject about the processing of PI if:

- the data subject already has the information (however, in this case, according to the Authority, the controller must be able to prove that the provision of information has already happened, that all necessary aspects of the data processing have been shared with the data subject and that there has not been any change in the processing);
- the provision of such information proves impossible or would involve a disproportionate effort;
- obtaining or disclosure is expressly laid down by EU or EU member state law to which the controller is subject and that provides appropriate measures to protect the data subject's legitimate interests; and
- when the PI must remain confidential subject to an obligation of professional secrecy regulated by EU or EU member state law, including a statutory obligation of secrecy.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

PI must be accurate and kept up to date where necessary. Inaccurate PI must be erased or rectified without undue delay. Healthcare is an exemption where the original inaccurate data must be kept in medical records.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The controller may not collect PI that is unnecessary or irrelevant for the purpose (data minimisation).

If the scope of PI is set by specific national law, then only that PI may be processed. Otherwise, the controller can decide on its own about the amount of PI, but it must be in line with the data minimisation principle.

Data retention

18 Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The controller may hold PI only until it is necessary for the purpose (storage limitation).

If specific national law sets the retention periods, those retention periods shall apply. If the law determines the circumstances of processing (such as the scope of PI and authorised persons) but not the duration of processing, the necessity of processing should be reviewed every three years. In other cases, the controller must decide on its own about the duration of processing, but it must be in line with the storage limitation principle.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI may only be processed for a specified, explicit and legitimate purpose. The Authority adds that the purpose needs to be as specific as possible (eg, 'marketing' is incorrect, as it allows different interpretations, 'sending newsletters' is correct as it allows only one interpretation). If the PI was collected for one purpose, in principle it should not be used for another purpose (finality principle).

Exceptions apply from the finality principle in the following cases:

- if the new processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- if the data subject gave consent to the processing for a different purpose; and
- if the processing for a new purpose is based on such EU or EU member state law that aims to achieve certain purposes (eg, home security or public safety) and the processing is necessary and proportionate to the purpose.

If none of the above applies, the controller may carry out a compatibility check according to the GDPR rules to check whether the old purpose is compatible with the new one.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Hungarian law does not have a specific, local restriction on the use of PI for making automated decisions (without human intervention). The general GDPR rule (article 22) applies according to which the data subject has the right not to be subject to a decision based solely on automated decision-making, including profiling.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The EU General Data Protection Regulation (GDPR) rules apply directly. The controller must implement measures that can prevent PI from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. When deciding about the appropriate measures, the controller must consider:

- the state of the art (as technology evolves constantly);
- the costs of implementation of the measures;
- the context of the data processing (eg, its nature, scope and purposes of processing); and
- the associated risks (arising from the data processing) for the rights and freedoms of data subjects.

The burden of deciding what measures are necessary to mitigate the risks is entirely on the controller. But the GDPR itself describes some measures that are advised to be implemented as appropriate:

- the pseudonymisation and encryption of PI;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to PI promptly in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing.

The controller is responsible for choosing processors that provide sufficient guarantees to implement adequate technical and organisational measures. To achieve this, the controller must conclude a data processing agreement.

For organisations falling under the scope of Act L of 2013 on the electronic information security of state and local administrative bodies (the Information Security Act), a stricter set of rules applies. Such organisations are placed into one of five categories, depending on the severity of the possible security breach. The categories will require different levels of data security.

Last, the implementation of Directive (EU) 2016/1148 on network and information security (the NIS Directive) also imposes stricter cyber rules for organisations that fall under its scope (ie, online marketplaces, search engine providers and cloud service providers).

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

If a data breach presents a risk to the rights and freedoms of natural persons, the controller must report it to the National Authority for Data Protection and Freedom of Information (the Authority) within 72 hours of gaining knowledge of the data breach. The processor should be obliged in the data-processing agreement to notify the controller about the breach promptly so that the controller can meet the 72-hour deadline.

The controller must also notify the affected natural persons if the processing will likely result in a high risk for the rights and freedoms of those people (eg, physical, material or non-material damages).

Irrespective of whether the notification threshold is reached, the controller must document all relevant information about data breaches. It is also advisable to retain any documentation as proof that the data breach has been handled adequately.

Apart from this general regime, there are some Hungarian sector-specific notification rules:

- providers of electronic communication service must also notify the Hungarian Telecommunication Authority within 24 hours of learning of the breach, and provide a second notification within 72 hours;
- organisations falling under the scope of the Information Security Act must report security incidents (including data breaches) promptly to the central incident management centre (defined in the Information Security Act); and
- organisations falling under the scope of the NIS Directive must report security breaches (including data breaches) that have a

substantial impact on the provision of a service that they offer within the European Union.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

A lack of implementation of internal control does not automatically lead to EU General Data Protection Regulation (GDPR) sanctions, but it is highly recommended. This is because, in the lack of such controls, it would be very difficult to ensure and demonstrate compliance with the GDPR requirements.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

It is not mandatory to appoint a data protection officer unless:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale special categories of PI and PI relating to criminal convictions and offences.

The data protection officer's role is mainly supportive and controlling. The officer's primary responsibilities are:

- to inform and advise the controller or the processor and the employees who carry out processing about their obligations under data protection laws;
- to monitor compliance with data protection laws (eg, collecting information about processing, checking the compliance of processing and issuing recommendations on compliance);
- to provide advice on the data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing; and
- to assist in maintaining the records of processing activities (although not an explicit legal obligation, it is recommended as best practice).

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Both controllers and processors are required to maintain the internal records of processing (ROP) under article 30 of the GDPR. An exemption from this obligation applies in the case of an organisation employing fewer than 250 persons, but only if:

- the processing is occasional (which is rare);
- the processing does not result in a risk to the rights and freedoms of data subjects; and
- sensitive PI or PI relating to criminal data are not processed.

As ROP gives an overall picture of the data processing of an organisation in terms of compliance, the National Authority for Data Protection and Freedom of Information (the Authority) may start an investigation by asking for it.

As under the accountability principle, the controller must be able to demonstrate compliance with data protection legislation, it is also advisable to implement internal data protection policies as well as other documentation (eg, privacy policies, legitimate interest tests and consent forms).

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Controllers must undertake a privacy impact assessment (PIA) in relation to certain uses of PI to mitigate the risks arising from high-risk data processing. The Authority published a list of typical cases in which a PIA is required (eg, large-scale profiling or systematic monitoring). Controllers may decide on the PIA methodology on their own, but the Authority recommends the Hungarian version of the French data protection authority's PIA software.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

New GDPR processing rules apply in Hungary, which include:

- privacy by design: controllers must consider the key data protection concern issues such as pseudonymisation or data minimisation via appropriate technical and organisational measures in the early stages of the processing (at the time of deciding on processing) and through the whole life cycle of the data processing; and
- privacy by default: controllers must take appropriate measures so that data processing by default is limited only to a strictly necessary extent, particularly regarding the amount of PI collected, the duration of the processing and access rights.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Controllers or processors are not required to register their data processing with the National Authority for Data Protection and Freedom of Information (the Authority). This obligation ceased in Hungary when the EU General Data Protection Regulation entered into force.

Other transparency duties

29 | Are there any other public transparency duties?

There are other public transparency duties, such as:

- notification of the Authority about the data protection officer's contact details; and
- sector-specific transparency obligations, such as the obligation of the employer to disclose its whistle-blowing operation on its website or the CCTV operators' obligation to place an adequate camera sign.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The rules on the transfer of PI depends on the qualification of the service provider:

- if the service provider acts solely based on the transferor's instructions it will be qualified as a processor. In such case, the transferor must conclude with the service provider a data-processing agreement, under EU General Data Protection Regulation (GDPR) rules. The data subject must be notified about the essential details of such processor (eg, its name, location of processing and type of processing activity);
- if the service provider decides on an important outsourced function on its own independently it may be qualified as a controller. In such case, transfer of PI must be based on proper legal ground and the data subject must be notified about the details of such transfer; and
- if the service provider decides on an important outsourced function jointly with the transferor, a joint controllership agreement must be concluded and the essence of the agreement must be made available to data subjects.

The main legal grounds include:

- the data subject's consent;
- the necessity for the performance of a contract (to which the data subject is party or to take steps at the request of the data subject before entering into a contract);
- the necessity for compliance with a legal obligation to which the controller is subject (Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information adds that such legal obligation must be set out in an act of the parliament or a municipal decree);
- the necessity to protect the vital interests of the data subject or another natural person;
- the necessity for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; and
- the necessity for the legitimate interests of the controller or by a third party.

Restrictions on third-party disclosure

31 Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Under the Hungarian data protection practice, disclosure of PI (ie, providing PI access to several persons) is prohibited, unless the data subject gives his or her consent or the PI relates to public affairs (eg, the PI relates to the exercising of a public function of a person, and not his or her private life).

Controllers must take measures that, by default, PI cannot be accessed by natural persons without the intervention of the individual identified. Unauthorised disclosure of PI may qualify as a data breach.

Cross-border transfer

32 Is the transfer of PI outside the jurisdiction restricted?

PI may only be transferred outside the European Economic Area to countries that provide an adequate level of protection according to the decisions of the European Commission (eg, Canada or Japan). In the case of other non-EEA countries, the transfer of PI is permitted only if it is based on appropriate data protection safeguards or if a derogation applies.

Safeguards may include the following legal instruments:

- standard contractual clauses (SCCs) approved by the European Commission;
- binding corporate rules (BCRs) for transfers within international company groups;
- a code of conduct that is officially approved according to GDPR rules;
- a certification mechanism that is officially approved according to GDPR rules; and
- an individual transfer agreement approved by the National Authority for Data Protection and Freedom of Information (the Authority).

The *Schrems II* decision (case C-311/18) of the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield legal framework in the case of transfers to the United States and in general made transfers of PI outside the European Economic Area more complicated.

The CJEU made it clear that it is not sufficient just to rely on the paperwork in the context of safeguards (eg, just signing the SCC). The controller must factually assess and document to establish if the level of protection required by EU law is respected in the third country before determining whether the guarantees provided by the safeguards (eg, by the SCCs or BCRs) can be complied with in practice (eg, whether the access to PI by public authorities is not a disproportionate measure). If not, the controller must assess whether by providing supplementary measures the adequate level of protection can be met (eg, by the encryption of PI, which would make the access to PI by public authorities meaningless).

If an adequate level of protection could not be met, the controller may still transfer the PI, if any derogations apply. Derogations may be:

- the data subject gives his or her explicit, specific and informed consent to the transfer;
- the transfer is objectively necessary for the performance of the contract with the data subject;
- the transfer is necessary to protect the vital interests of an individual;
- the transfer is necessary for the public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and
- the transfer is necessary for compelling and overriding legitimate interests of the controller (under limited conditions such as the transfer is not repetitive and apply only to a limited number of data subjects).

The scope of these derogations is specified in European Data Protection Board Guideline No. 2/2018.

Further transfer

33 If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The cross-border transfer rules equally apply to every form of transfer, irrespective of whether it is a controller-controller, a controller-processor or an onward transfer.

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No, in general the law does not require PI or a copy of PI to be retained in Hungary. However, certain organisations falling under the scope of the

Information Security Act (such as certain public bodies and data processors of certain public records) must retain data in Hungary and may not transfer it to other countries. Similarly, data localisation requirements apply to online betting service providers according to the Gambling Act.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals may ask the controller to obtain a copy of their personal information or to obtain supplementary information about the processing of their personal information.

Individuals do not have to justify why they want to exercise their right to access. However, certain limitations still apply to this right:

- the controller may request the individual to identify himself or herself if, for example, the request is submitted orally or by email, but the controller has reasonable doubts about the identity. If the individual does not identify himself or herself, the controller may refuse the request;
- the controller may request the individual to specify his or her request;
- the controller may refuse the request if it is manifestly unfounded or excessive (but, according to the National Authority for Data Protection and Freedom of Information (the Authority), in both cases the controller may not refuse the request if the administrative cost of fulfilling the request is trivial); and
- the right to access may not adversely affect the rights and freedoms of others (eg, PI of other data subjects or trade secrets).

Other rights

36 | Do individuals have other substantive rights?

Individuals have other substantive rights under the EU General Data Protection Regulation (GDPR) framework. Individuals may:

- request the erasure of the PI in some circumstances (if, eg, the PI is no longer necessary for the purpose);
- request the rectification of the PI, if the PI is inaccurate or incomplete;
- the restriction of the PI, meaning that the controller may only store the PI (if, eg, the PI is no longer necessary for the purpose, but the data subject needs it for legal claims);
- object to the data processing, if the processing is based on legitimate interest and the data subject's interest overrides the interest of the controller;
- the exporting of their PI (ie, receiving the PI in a portable format or directing the controller to transmit the PI to another controller); and
- not be subject to decisions based solely on automated decision making.

Individuals have the right to damages should a controller breach their rights under the GDPR.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals may claim both material damages covering the actual damage and non-material damages covering injury to feelings. Controllers and processors must be able to prove that the breach of data protection laws has not occurred.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals may claim damages only in front of the court, but other rights may be enforceable in front of both the Authority and the court.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Data Protection Act) establishes the possibility of exercising some data subject rights (ie, the rights of access, rectification, erasure, restriction of the processing and to object) on behalf of deceased persons. Five years after the death of the data subject, the close relative or the authorised person of the data subject may exercise certain data subject rights under the conditions set out in the Data Protection Act.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The National Authority for Data Protection and Freedom of Information (the Authority) issued some guidance about using cookies. The most important rules are the following:

- the user must be informed about the cookies. Practically, a pop-up message should appear during the first visit to the website, which should contain the link in which the full information about the cookie is accessible;
- non-functional cookies, which are not essential for the website operation, such as marketing or analytical cookies, shall be placed on the user's device only based on the user's prior informed and explicit consent;
- functional cookies, which are essential for the website's operation (eg, without them the communication through the website would not work) may be placed on the user's device without his or her consent. But a legitimate interest test must be conducted to prove that the website operator's interest in placing the cookies is stronger than the user's privacy interest; and
- the website operator is liable for the third-party cookies on its website; thus it should use only those third-party cookies that it has full knowledge of.

The European Data Protection Board (EDPB), in its recently updated guidance on consent (Guidelines 05/2020 on consent), adds that the use of access to services and functionalities must not be made conditional on the consent for the use of cookies (which means that cookie walls are not acceptable). In January 2021, the Authority also stated how the website operators shall use embedded social media modules on their website. As website operators process personal data of users, by embedding tracking pixels (as this process enables the transfer of users' personal data to the social media provider), the Authority requires website operators to comply with the prior privacy notice and free

consent requirements. The Authority relies on EDPB Guidelines 08/2020 on the targeting of social media users.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Under the Hungarian law on advertising, sending unsolicited electronic marketing (via email, fax or text) is permissible only if the prior, explicit and unambiguous consent of the recipient has been obtained. However, the Authority, in its guideline, recognised that based on the EU General Data Protection Regulation it is permissible to send direct marketing communication if:

- it is directed at existing clients;
- it relates to similar products and services;
- the client has the possibility to opt out from future communication; and
- the sender performs and documents the legitimate interest test in which it explains why its business interest overrides the client's interest.

In the case of voice-to-voice calls, an individual may be called only if he or she has not objected to such communication (eg, in the relevant publicly available phone directory there is no indicator showing that the person does not wish to receive marketing calls). In the case of automated calls, the holder of the phone number must give his or her prior explicit consent to receive the call (eg, in the phone subscription contract).

Targeted advertising

42 | Are there any rules on targeted online advertising?

The GDPR is directly applicable; there is no specific local requirement.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The Authority argues that, in the case of holding special categories of PI, apart from having one of the six legal grounds above, the controller must also check whether one of the conditions of article 9 of the GDPR applies (eg, the data subject needs to give explicit consent or the processing needs to be necessary to exercise or defend legal claims).

Profiling

44 | Are there any rules regarding individual profiling?

The GDPR is directly applicable; there is no specific local requirement.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There is no specific Hungarian legislation explicitly regulating cloud computing, and the Authority has no guidance about it either. Controllers, however, are advised to adhere to European Commission best practices (eg, article 29 of the Data Protection Working Party Opinion on Cloud Computing).

Further, the Central Bank of Hungary (CBH) issued guidance (effective from 1 May 2019) on how financial institutions should use social and public clouds. The guidance, among others, contains rules on the minimum elements of cloud service agreements, risk analysis, implementation of cloud systems, control mechanisms, exit strategy and notification to the CBH.

VJT & PARTNERS

Endre Várady
varadye@vjt-partners.com

János Tamás Varga
vargajt@vjt-partners.com

Andrea Belényi
belenyia@vjt-partners.com

Kernstok Károly tér 8
1126 Budapest
Hungary
Tel: +36 1 501 9900
www.vjt-partners.com

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The National Authority for Data Protection and Freedom of Information (the Authority) recently imposed its record EU General Data Protection Regulation (GDPR) fine of 250 million forints against a bank for its improper automatic AI analysis of recordings of customer service calls. The Authority, among others, found that the bank did not address the proportionality of the data processing and its potential risks and that data subjects did not get meaningful information about the voice analysis. The case could be important for similar AI technologies used across the Hungarian market.

India

Arjun Sinha, Mriganki Nagpal, Siddhartha Tandon and Prakriti Anand

AP & Partners

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Currently, India does not have a comprehensive legal framework for data protection. The Information Technology Act 2000 (the IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 framed under the IT Act regulate the collection, use, processing and transfer of personal data and sensitive personal data in India.

Additionally, sector-specific regulators also govern data collection, use and processing activities.

The Ministry of Electronics and Information Technology has framed draft privacy legislation, the Personal Data Protection Bill 2019 (the PDP Bill). The PDP Bill is modelled on Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) of the European Union and seeks to protect the personal data of individuals and establish a data protection authority to regulate all personal data-related activities within India. The PDP Bill was tabled in Parliament and (as is customary for key legislation) was then reviewed by the Joint Parliamentary Committee comprising of members of both houses of Parliament.

However, news reports indicate that the PDP Bill has been shelved by the government and may be rewritten. In recent discussions with the industry, the Minister of Electronics and Information Technology stated that the IT Act is in the process of being rewritten and will be released this year.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The IT Act does not establish a regulator to oversee the implementation of data protection (similar to a data protection authority under the GDPR).

However, under section 70B of the IT Act, the government has established the Computer Emergency Response Team (CERT-In) to analyse, forecast and respond to cybersecurity incidents (which include unauthorised access, disruption and use of a computer resource). The CERT-In is empowered to investigate data breaches, and non-compliance with directions of the CERT-In has financial and criminal penalties. Additionally, the Reserve Bank of India also intends to establish the financial sector-specific Computer Emergency Response Team (CERT-Fin). However, CERT-Fin is yet to be made operational.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

No, there are no express legal obligations to cooperate with foreign data protection authorities.

However, foreign data protection authorities that need assistance in conducting criminal investigations in India can do so under the provisions of the Code of Criminal Procedure 1973. Here, the government has executed mutual legal assistance treaties with foreign governments to assist with the service of summons, warrants and judicial processes in India and abroad.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Yes, a data breach can lead to an administrative order or criminal penalties. Under section 43A of the IT Act, negligence in implementing the security standards can lead to compensation claims from affected users.

Separately, data breaches are required to be reported to the CERT-In by both foreign and domestic entities. Failure to report this information may result in financial penalties of 25,000 Indian rupees (under section 45 of the IT Act). Further, failure to comply with information requests by the CERT may result in financial penalties of 100,000 rupees and imprisonment of one year.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

India does not currently have a data protection authority.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Transfers of sensitive personal data to government agencies or third parties on directions of a court or a government body, or under a legal obligation, do not require the consent of the user.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Yes, various Indian legislation deals with the issue of interception of communications, electronic marketing or monitoring as well as surveillance of individuals.

Interception, monitoring and surveillance powers of the state

Sections 69 and 69B of the Information Technology Act 2000 (the IT Act) empower the government to monitor or decrypt information in certain circumstances such as for national security, an emergency or in the interest of public safety. Further, criminal legislation such as the Code of Criminal Procedure 1973 under section 91 and anti-terror legislation such as the Unlawful Activities (Prevention) Act 1967 empower law enforcement authorities to demand the production of electronic documents and carry out related surveillance or interception activities.

Telecom service providers, such as carriers and internet service providers, are required to assist government agencies in the interception of communications through their network and facilitate government monitoring and interception requests under the terms of their licence and under the Indian Telegraph Rules 1951.

These monitoring and interception activities can be carried out by various arms of the government such as the Intelligence Bureau, the Enforcement Directorate, the Central Bureau of Investigation, state police and tax authorities, among others.

Electronic marketing

Any marketing or advertising activities that constitute an unfair trade practice (eg, false advertising and deceptive pricing) carry financial penalties under the Consumer Protection Act 2019.

Additionally, the telecom regulatory authority of India regulates marketing via texts and voice calls through the Telecom Commercial Communications Customer Preference Regulations 2018 (TCCCPR). The TCCCPR requires consent for marketing via texts and voice calls. Non-compliance with the TCCCPR can result in a financial penalty of up to 5 million Indian rupees per month.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

In addition to the obligations under the IT Act, data is also subject to certain sectoral regulations:

- Cross-border transfers of geospatial data are restricted as per the Guidelines for Acquiring and Producing Geospatial Data and Geo-spatial Data Services including Maps.
- Payment data collected by payment systems providers (eg, wallets, payment gateways and banks) is subject to data localisation requirements imposed by the Reserve Bank of India (RBI). Further, the RBI's Digital Payment Security Control Directions 2020 also provide a governance framework and security standards for digital payments data.
- The Medical Council of India's Telemedicine Guidelines place an obligation on 'registered medical practitioners' to maintain their patients' privacy and confidentiality.
- Insurance-related data is regulated in terms of the Insurance Regulatory and Development Authority of India's Guidelines on Information and Cyber Security for Insurers. Insurance companies must ensure the confidentiality of their policyholders' information and adequate security measures for their electronic systems. Further, this data must be stored locally. Any data outsourced to third-party service providers should also have adequate security protocols to ensure the confidentiality of the policyholders.
- The unified licence agreement entered into by a telecom service provider with the government regulates the storage and transfer of subscriber information.
- The Indian Companies Act 2013 mandates corporate entities to store their register of members and debenture holders and annual financial statements at their registered office in India. However, copies of this information may be stored overseas.

PI formats

9 | What categories and types of PI are covered by the law?

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the RSP Rules) classify data into personal and sensitive personal information:

- PI is defined as any information that can be used either directly or indirectly (ie, in combination with other data available or likely to be available) to identify a natural person; and
- sensitive personal information (SPI) is defined as personal information related to passwords, financial information (including account details and card data), physical and mental health information or biometric information. However, information that is freely available or accessible in the public domain or furnished under the Right to Information Act 2005 or any other applicable law is excluded from being considered as SPI.

Generally, PI has limited regulation under the RSP Rules, restricted to providing a privacy policy, appointing a grievance redressal officer and instituting reasonable security practices to protect such data.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The IT Act provides for specific instances of extraterritorial application. Under section 75 of the IT Act, the IT Act applies to offences and contraventions committed outside India if such action relates to a computer, computer system or network in India.

Further, a notification dated 24 August 2011 by the Ministry of Electronics and Information Technology clarifies that the RSP Rules apply to body corporates and persons located in India. This would include the data of individuals located in India and held by Indian body corporates but stored overseas (eg, offshore cloud service providers).

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

No, under Indian data protection law a distinction is drawn between SPI and PI. The collection, disclosure and transfer of SPI are regulated under the RSP Rules whereas the processing of personal information is outside the scope of the RSP Rules.

The RSP Rules do not define the concepts of the data owner, data controller and data processor. Instead, the RSP Rules provide for 'body corporate' or 'provider of information'. A body corporate is an entity that handles data, and the provider of the information is a natural person that provides sensitive and personal data to a body corporate. Under the RSP Rules, a natural person has certain rights, while duties relating to

the data collected, processed or transferred are imposed on such body corporates.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the RSP Rules) set out specific conditions on the collection, processing and transfer of sensitive personal information (SPI). These are:

- any SPI must be collected for lawful and necessary purposes;
- before collection, the organisation must obtain specific written consent from the individual providing the SPI. The individual must also be given notice of the purpose of collection and the intended recipients of the SPI; and
- transfers of SPI outside India can only be made after ensuring that the receiving entity or its jurisdiction has the same level of protection as required under Indian law, and only if the transfer is necessary to perform a lawful contract. However, cross-border transfers of personal information are not restricted by the RSP Rules.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Yes, the RSP Rules impose stringent obligations on the processing of SPI. Also, sector-specific regulations place an additional burden on the processing of certain forms of SPI.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the RSP Rules) require entities to notify individuals whose PI and SPI they are collecting and notify individuals of its practices and policies with respect to PI and SPI in a privacy policy document that must be made available on its website.

Further, specifically in the case of SPI, in addition to the requirement under Rule 4 of the RSP Rules, Rule 5(3) of the RSP Rules stipulates that an entity collecting data should notify an individual:

- that information is being collected;
- the purpose for which information is being collected;
- of the intended recipients of the information; and
- the name and address of the agency that is collecting the information and will retain the information.

Under Rule 5(7) of the RSP Rules, entities must also notify individuals prior to collecting any SPI. The notice must also provide an option to the provider of the information not to provide the SPI sought to be collected. However, it is legitimate to deny services on the revocation of consent.

Exemptions from transparency obligations

15 | When is notice not required?

Rule 6(1) of the RSP Rules exempts the notice or consent for transfers of SPI to notified government agencies or any third party by order from a court, tribunal or government agency.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

The RSP Rules provide an ability to demand corrections. However, a body corporate is not responsible for the authenticity of the information provided to them by individuals.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

No, there are no restrictions on the type or volume of PI that may be collected. However, the RSP Rules only stipulate that an entity should not hold SPI for a duration longer than required for purposes for which such SPI may lawfully be used or is required under any other law in force. Further, entities must only collect SPI that is necessary for the identified purposes, imposing limited data minimisation obligations.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

There are no restrictions on the length of time PI may be held by a body corporate. However, under Rule 5(4) of the RSP Rules, SPI should not be stored by an entity for longer than is required for the purposes for which the information may be used (or as required under any other law).

On the other hand, PI may be required to be held by an entity for a minimum time period under various regulations. For example, any intermediary (similar to a platform protected by safe harbour protections under US law) must store user registration information for a period of 180 days after the deletion of the user's account.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

While there are no restrictions on PI per se, the purposes for which SPI can be used by entities are restricted. As per Rule 5(2) of the RSP Rules, SPI must be utilised for the purposes for which they were collected. Any additional purpose requires additional consent from the individual from whom the data was collected.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Presently, there are no such express restrictions on the use of automated decision-making tools.

However, social media platforms are required to periodically review any automated tools used by them to detect and remove content that promotes rape and child sexual abuse, etc, on their platform.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the RSP Rules) require a body corporate to institute reasonable security practices and procedures and set out such practices in its privacy policy. Further, the body corporate must have a comprehensive and documented information security policy that contains managerial, technical, operational and physical security control measures.

Further, sector-specific regulations also set out security obligations on processing data. For example, the Reserve Bank of India (RBI) sets out standards for the protection of payments data. The RBI's regulations advise entities to adhere to payment standards over and above the payment card industry data security standard and payment application data security standard.

Similarly, the Insurance Regulatory and Development Authority of India requires insurance companies to ensure that the system in which the policy and claim records are maintained have adequate security features, and records pertaining to policies and claims are held in data centres located and maintained in India.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Yes, there is a legal requirement to notify the Computer Emergency Response Team (CERT-In) of certain 'cybersecurity incidents', which includes data breaches.

CERT-In has described a data breach as an incident where information is taken or stolen without authorisation or knowledge of the system's owner.

Any cybersecurity incident (including a data breach) that meets the following criteria must be reported within six hours:

- cyber-incidents and cybersecurity incidents of a severe nature (such as denial of service, distributed denial of service, intrusion or ransomware) on public information infrastructure;
- data breaches or leaks;
- large-scale or frequent incidents such as intrusion into computer resources and websites, etc; or
- cyber-incidents impacting the safety of human beings.

Failure to report these cybersecurity incidents (including data breaches) may result in financial penalties of up to 25,000 Indian rupees (under section 45).

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Yes, collectors and processors of PI are required to comply with 'reasonable security practices' in relation to PI. This includes having in place a comprehensive documented information security programme and information security policies. Compliance with the ISO 27001 standard is considered compliance with the above requirements.

Entities that do not comply with the ISO 27001 standard are required to conduct a periodic audit from an auditor empanelled with the government.

While there is no specified manner of demonstrating compliance in general, in case of a 'cyber security incident', companies can be required by government agencies (such as the Computer Emergency Response Team (CERT-In)) to demonstrate compliance of their internal security practices with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the RSP Rules).

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The RSP Rules require organisations to appoint a grievance officer to address discrepancies and grievances of individuals who provide information (personal information, non-personal information or sensitive personal information) to any company. The grievance officer must respond to grievances of individuals within 30 days of notice. The name and contact details of the grievance officer must be set out in the privacy policy of the company.

However, there are no particular criteria related to, for example, residence or employment status for the appointment of this data protection officer or grievance officer.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The RSP Rules require body corporates to draft and publish a privacy policy that specifies the data being collected, the purpose for which the data is being collected, disclosure of data collected to third parties and documents its information security policy containing managerial, technical, operational and physical security control measures for the protection of information.

Organisations (both foreign and domestic) are also required to maintain logs of their ICT systems and provide them to CERT-In on notice.

The logs must be maintained in India. Copy of logs can also be stored outside India as long as the organisation is able to provide CERT-In with the log data in a reasonable time.

Further, entities such as data centres, virtual private server providers, cloud service providers and virtual private network services other than those provided to corporate or enterprise customers are required to preserve customer information for at least five years after any cancellation or withdrawal of registration.

Ancillary legislation such as the Companies Act 2013 and the Income Tax Act 1961 also impose data retention and record-keeping obligations on certain personal information. For example, the Companies Act 2013 requires body corporates to maintain (in physical or electronic form) a register of members, directors, related parties and employee stock options, among others. Organisations also must retain financial data (payment to employees, consultants, loans received from individuals and shared capital information) for tax and audit purposes for seven years.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

No, there is no express requirement for conducting risk assessments in general. However, the RSP Rules specify that while transferring SPI outside the country, the data transferor must ensure that the recipient of the data provides the same level of protection as required under the RSP Rules.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

No, there are no obligations under the RSP Rules in relation to the design of PI processing systems.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

No, owners or processors of PI are not required to register with the supervisory authority.

There is no registration obligation for owners or processors of PI.

Other transparency duties

29 | Are there any other public transparency duties?

Entities that collect, receive, possess, store or handle personal information must have a privacy policy that sets out details such as the information collected, reasonable security practices instituted, and the name and contact number of the appointed grievance officer.

The privacy policy must be published on the website of the entity and be easily accessible by all users.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Outsourcing service providers are exempt from the consent and disclosure obligations under Rules 5 and 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the RSP Rules). However, they are still required to:

- set out a clear and easily accessible privacy policy;
- appoint a grievance officer; and
- institute reasonable security practices, such as the ISO 270001 standard specified under the RSP Rules.

Further, when such outsourcing service providers make overseas transfers of the data of persons located in India, they must ensure that the receiving entity provides the same level of protection as required under Indian law.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The RSP Rules restrict the non-consensual publication of sensitive personal information (SPI) by a body corporate, or the further disclosure of SPI by third parties. However, such SPI may be disclosed (without consent) to a notified government agency or third parties by order from a court, tribunal, or government agency.

Recent amendments to the Customs Act, 1962 restrict the publication of personal information of exporters and importers that is submitted to the customs department.

The Insurance Regulatory and Development Authority of India (IRDAI) also requires insurance companies to ensure that data is outsourced to third-party service providers who have adequate security policies. Insurance companies are also required to ensure that the data shared is not re-used by the service provider once the contract is concluded.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

While cross-border transfers of PI are not restricted, SPI can only be transferred outside India after ensuring that the receiving entity has the same level of protection as required under Indian law. Further, any such transfer should take place only if required for the performance of a lawful contract or with the consent of the individual.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

There are no government authorisations required for transfers of PI. Further, transfers to a third party, within or outside India, can be undertaken without consent, if carried out to perform a lawful contract.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

While there is no general local storage obligation under the RSP Rules, certain specific regulators impose localisation obligations. For example:

- the Reserve Bank of India (RBI) requires the storage of payment data (including customer data and transaction details) in India;
- the Department of Telecommunications requires the localisation of customer data by telecom companies;
- the IRDAI mandates local storage of insurance-related records, including records of all policies issued and claims made in India;
- companies registered in India are required to store their annual returns, registers of members and debenture holders at their registered office in India; and
- the recent Computer Emergency Response Team directions require organisations to maintain logs of all their IT systems in India for a rolling period of 180 days.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, individuals have the right to access sensitive personal information (SPI) held by entities.

Other rights

36 | Do individuals have other substantive rights?

Yes, under Rule 5(6) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, an individual can request an entity to review any SPI provided by them. Further, the individual can correct or amend any inaccuracies or deficiencies to such SPI.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes, negligence in implementing the security standards can lead to compensation claims from affected users under section 43A of the Information Technology Act 2000 (the IT Act). However, the law does not prescribe the maximum penalty payable.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Any claims under the IT Act to the value of 50 million Indian rupees or less are required to be heard by an adjudicating authority (an officer appointed by the central government). Claims greater than 50 million Indian rupees are heard by the Telecom Dispute Settlement and Appellate Tribunal (TDSAT). Decisions of the TDSAT can subsequently be appealed at the appropriate high court.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the RSP Rules) only apply to body corporates (ie, any company including a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities) and therefore excludes government agencies.

Further, the RSP Rules exempt the need for notice and consent for transfers to notified government agencies or to any third party by an order under the law for the time being in force.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The Information Technology Act 2000 (the IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the RSP Rules) do not directly cover the use of cookies or its equivalent technology. However, section 43 of the IT Act is widely worded and restricts accessing, downloading, copying or extracting 'any data', computer database or information from any computer, computer system or computer network without the permission of the owner or the person in charge. The use of the words 'any data' is interpreted to indirectly deal with the use of cookies or equivalent technology.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Marketing or promotional activities through voice calls and text, must be compliant with the Telecom Commercial Communications Customer Preference Regulations 2018 (TCCCPR). Telemarketing entities can only conduct marketing activities after registering themselves with their telecom carriers in compliance with the TCCCPR.

Under the TCCCPR:

- transactional communication (eg, one-time passwords or transaction details) does not require consent from the user. However, marketing activities require the implied or explicit consent of users;
- individuals can register with a 'do not disturb' registry. On registration, sending promotional or marketing messages without the consent of the recipient results in levy of financial penalties; and
- the TCCCPR also provides for a complaints mechanism and penalties for contravention of the regulations. Communication over email or instant messaging apps is not covered by the TCCCPR.

There are no specific regulations governing commercial communications sent via email or through messaging platforms (such as WhatsApp).

Targeted advertising

42 | Are there any rules on targeted online advertising?

While behavioural advertising is not restricted, significant social media intermediaries (ie, social media platforms with more than 5 million registered users) are required to inform a user if the information displayed on the platform is advertised, marketed, sponsored, owned or exclusively controlled. The form of labelling is left to the discretion of the significant social media intermediary.

Indian advertisers also follow self-regulatory guidelines framed by the Advertising Standards Council of India (the ASCI Code) for digital advertising. The ASCI Code advises social media influencers (or published on their accounts) to label promoted or sponsored materials, and prescribes guidelines for advertising products such as alcohol, tobacco, real money gaming and cryptocurrencies.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The RSP Rules regulate the processing of certain sensitive categories of personal information such as financial information, medical records, biometric information and passwords, etc. The RSP Rules also require

entities to have comprehensive security and data policies in relation to such sensitive information and regulate its transfer and disclosure.

Profiling

44 | Are there any rules regarding individual profiling?

No, individual profiling is not currently regulated.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There is no specific legislation in India governing cloud computing services. However, section 43A of the IT Act read with the RSP Rules set out the regulatory framework for the creation, collection, storage, processing and use of electronic data (including personal and sensitive personal information recorded in electronic form) in India. Cloud computing services that deal with personal or sensitive personal information need to comply with the requirements set out under the RSP Rules.

Under the Computer Emergency Response Team (CERT-In) rules, data centres are required to maintain logs of their IT systems in India, which need to be provided to the CERT-In on the occurrence of a cybersecurity incident.

In addition to the IT Act and the RSP Rules, sector-specific rules provided by the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDAI) indirectly deal with cloud computing services in India. For example, the RBI's Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks 2006 makes it mandatory for banks and entities to which banks have outsourced their services to preserve and protect the security and confidentiality of customer information. These guidelines would also be applicable for offshore outsourcing of financial services by banks. Similarly, the IRDAI's Guidelines on Information and Cyber Security for Insurers require insurers using cloud computing services to have data protection processes and control in place.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Personal Data Protection Bill 2019 (PDP Bill), modelled on the Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) of the European Union has been pending before the Indian legislature since 2019 and has now been reviewed by the Joint Parliamentary Committee. However, news reports indicate that the government is considering shelving the PDP Bill and bringing in comprehensive legislation that covers both personal and non-personal data.

In October 2021, the Supreme Court constituted a three-member committee to deliberate on cybersecurity, laws relating to surveillance and privacy, and preventing the invasion of privacy by state and non-state entities.

Separately, on 28 April 2022, the Computer Emergency Response Team (CERT-In) issued directions relating to information security practices and reporting of cybersecurity incidents. Key obligations imposed by the CERT-In directions are as below:

- expand the types of cybersecurity incidents that must be reported;
- clarify that the reporting obligation applies to both domestic and overseas entities;
- impose a mandatory reporting timeline of six hours within the occurrence of the incident; and
- require storage of a copy of the log data in India.

AP & PARTNERS
ADVOCATES

Arjun Sinha
arjun.sinha@appartners.in

Mriganki Nagpal
mriganki.nagpal@appartners.in

Siddhartha Tandon
siddhartha.tandon@appartners.in

Prakriti Anand
prakriti.anand@appartners.in

B-62
Pashchimi Marg
Vasant Vihar
New Delhi - 110057
India
Tel: +91 11 4259 4444
www.appartners.in

Indonesia

Rusmaini Lenggogeni and Charvia Tjhai
SSEK Legal Consultants

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Indonesia has yet to enact a data protection regulation that would apply to PI. To date, Indonesia does not have in place a single and comprehensive law governing data privacy or data protection. The relevant provisions on the protection of privacy of PI are spread across various laws and regulations, namely:

- Law No. 11 of 2008 regarding Electronic Information and Transactions (21 April 2008), as amended by Law No. 19 of 2016 (25 November 2016) (the Electronic Information Law);
- Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019);
- Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016); and
- MOCI Regulation No. 5 of 2020 regarding Private Electronic Systems Providers (24 November 2020), as amended by Law No. 10 of 2021 (21 May 2021) (MOCI Regulation 5/2020).

The above laws and regulations are hereinafter collectively referred to as the PDP Regulations.

It is important to note that the government is preparing a Personal Data Protection Draft Bill (the PDP Draft Bill), which would recognise standard international concepts such as data controller, data processor, sensitive personal data, dedicated data protection officers and automatic processing once the PDP Draft Bill is enacted. As of the time of writing, however, the PDP Draft Bill has not been passed and is still being discussed at the House of Representatives. It was reported that the PDP Draft Bill was targeted for enactment by 2022.

Other than the above PDP Regulations, the protection of personal data is included in several sector-specific laws and regulations, though most of these laws and regulations only address data protection briefly. These are:

- Law No. 36 of 2009 regarding Health (13 October 2009), which stipulates that, in principle, every person is entitled to the confidentiality of their personal health information that has been provided to or collected by healthcare providers (the Health Law);
- Bank Indonesia Regulation No. 22/20/PBI/2020 regarding Bank Indonesia Consumer Protection (22 December 2020);
- Financial Services Authority (OJK) Regulation No. 1/POJK07/2013 regarding Financial Consumer Protection (6 August 2013), as last amended by OJK Regulation No. 18/POJK07/2018 (10 September 2018) (OJK Regulation 1/2013). OJK Regulation 1/2013 prohibits financial service providers from disclosing customer data or information to third parties without written consent from the customer or unless they are required to make such disclosure by law. Where a financial service provider obtains the data or personal information of a person or a group of persons from a third party, it is required to obtain written confirmation from the third party that the person or group of persons has agreed to the disclosure; and
- Law No. 36 of 1999 regarding Telecommunications (8 September 1999), which prohibits the tapping of information transmitted through telecommunications networks. Telecommunications service operators must maintain the confidentiality of any information transmitted or received by a telecommunications subscriber through a telecommunications network or telecommunications service provided by the respective operator.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

To date, there is no specific data protection authority that oversees data protection in Indonesia. Under the PDP Regulations, the MOCI is responsible for monitoring and regulating data protection.

To the extent of its investigative power, the MOCI also has the power to, among other things, organise and supervise information related to the transfer of personal data or impose administrative sanctions for violations of data protection regulations. However, for specific matters, such as a dispute related to the failure or breach of personal data protection, data subjects may submit a written complaint to the Directorate General of Application of Informatics (DGAI), part of the MOCI, within 30 business days from the discovery of the failure to protect the personal data of the data subject. If a violation is found, the DGAI may recommend that the MOCI impose certain administrative sanctions on the Electronic System Provider (ESP).

Also, certain other government agencies may oversee data protection for their respective sectors, such as the OJK for financial service providers and the Ministry of Health for healthcare providers.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

In general, the MOCI may cooperate with other data protection authorities, such as other governmental agencies, to follow up on complaints from data subjects regarding the failure to protect personal data. However, the MOCI has not entered into any cooperation agreements with foreign authorities.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Each of the PDP Regulations stipulates different sanctions. The Electronic Information Law regulates criminal sanctions, while GR 71/2019 and MOCI Regulation 20/2016 only stipulate administrative sanctions. The administrative sanctions under GR 71/2019 and MOCI Regulation 20/2016 also differ. Nonetheless, the following sanctions stipulated thereunder are equally enforceable by the MOCI:

- MOCI Regulation 20/2016 imposes administrative sanctions for breaches of data protection in the form of:
  - a verbal warning;
  - a written warning;
  - a temporary suspension of activities; or
  - an announcement on the MOCI website; and
- GR 71/2019 imposes administrative sanctions due to breaches of data protection in the form of:
  - a written warning;
  - an administrative penalty;
  - a temporary suspension of activities;
  - termination of access to the electronic system; or
  - the expulsion from the list of registered ESPs for the violation of certain provisions of GR 71/2019 relating to the protection of personal data.

If applicable, the imposition of the above administrative sanctions does not eliminate criminal and civil responsibilities.

Criminal sanctions, which can be imposed on both corporations and individuals, may also apply as follows:

- fines of 600 million rupiah to 800 million rupiah or four to eight years' imprisonment for unlawful access;
- fines of 800 million rupiah to 1 billion rupiah or six to 10 years' imprisonment for interception or wiretapping of a transmission;
- fines of 2 billion rupiah to 5 billion rupiah or eight to 10 years' imprisonment for the alteration, addition, reduction, transmission, tampering, deletion, moving or hiding of electronic information or electronic records; and
- fines of 10 billion rupiah to 12 billion rupiah or 10 to 12 years' imprisonment for the manipulation, creation, alteration, destruction, or damage of electronic information or electronic documents with a purpose of creating an assumption that such electronic information or documents are authentic, and other violations related to the processing of electronic information or documents.

Criminal proceedings are initiated by the Indonesian police and prosecutors.

Judicial review of data protection authority orders

5 Can PI owners appeal to the courts against orders of the data protection authority?

In general, the PDP Regulations do not provide specific rules for appeal to the courts against orders of the data protection authority. However, according to the PDP Regulations, in general, PI owners have the right to file a lawsuit or claim for damages if their rights related to PI under the relevant laws and regulation are infringed.

SCOPE

Exempt sectors and institutions

6 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The current PDP Regulations are rather broad, as can be seen from the definition of an Electronic System Provider (ESP). An ESP is defined as every person, state administrator, business entity and community providing, managing, or operating an electronic system, either individually or jointly, for electronic system users, for their personal purpose or another party's purpose. The term 'electronic system' is defined as a set of electronic devices and procedures that function to prepare, collect, process, analyse, retain, display, publish, transmit or disseminate electronic information. The Minister of Communication and Informatics (MOCI) has interpreted this to mean that any person or entity that stores data electronically is considered an ESP using an electronic system that should be subject to the PDP Regulations.

ESPs are further divided between private scope ESPs and public scope ESPs, as further defined below:

- private scope ESPs: MOCI Regulation No. 5 of 2020 regarding Private Electronic Systems Providers (24 November 2020), as amended by Law No. 10 of 2021 (21 May 2021), defines private scope ESPs as individuals, business entities and communities that provide electronic systems; and
- public scope ESPs: GR 71/2019 defines public scope ESPs as state administrative agencies, legislative, executive and judicial institutions at the central and regional government level and other agencies that are formed by virtue of laws and regulations, and institutions appointed by state administrative agencies. The latter refers to institutions providing an electronic system with a public scope on behalf of the appointing state administrative agency.

GR 71/2019 excludes public scope ESPs that have regulatory and supervisory authority in the financial sector.

Interception of communications and surveillance laws

7 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

First, an interception of communication is generally governed by Law No. 11 of 2008 regarding Electronic Information and Transactions (21 April 2008), as amended by Law No. 19 of 2016 (25 November 2016) (the Electronic Information Law), which stipulates that any interception or wiretapping of a transmission shall be subject to criminal sanction in the form of a maximum fine of 800 rupiah million and up to 10 years' imprisonment. However, exemptions apply for lawful interception or wiretapping of a transmission in the framework of law enforcement, such as in a corruption case investigation.

Second, concerning electronic marketing or monitoring and surveillance of individuals, if such action is conducted using electronic means, then it must comply with personal data protection principles and relevant rules under the PDP Regulations.

Other laws

8 Are there any further laws or regulations that provide specific data protection rules for related areas?

The PDP Regulations do not regulate this matter. We are also not aware of any specific regulations on employee monitoring. In this regard, considering that the concept of employee monitoring is not recognised under the PDP Regulations or any other Indonesian laws or regulations,

and to the extent the employer qualifies as an ESP and processes the personal data of employees, who may be considered data subjects, consent is required.

For e-health records, Law No. 36 of 2009 regarding Health (13 October 2009) stipulates that, in principle, every person is entitled to the confidentiality of their personal health information that has been provided to or collected by healthcare providers. This personal health information shall be considered personal data. Concerning the use of social media, it shall also be subject to the data protection requirements under the PDP Regulations as they pertain to user consent for the collection and processing of personal data.

Last, credit card information is considered confidential information in the banking sector. Financial Services Authority (OJK) Regulation No. 1/POJK07/2013 regarding Financial Consumer Protection (6 August 2013), as last amended by OJK Regulation No. 18/POJK07/2018 (10 September 2018) (OJK Regulation 1/2013), prohibits financial service providers from disclosing customer data or information to third parties unless they receive written consent from the customer or are required to make such disclosure by law.

PI formats

9 | What categories and types of PI are covered by the law?

The definition of personal data has evolved throughout the enactment of the PDP Regulations. MOCI Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) defines personal data as certain personal data that is stored or cultivated, with its accuracy maintained and confidentiality protected. GR 71/2019 further defines personal data as any data relating to a person that is identified or is self-identifiable, or is combined with other information, directly or indirectly, through electronic and non-electronic systems. The current regulatory framework does not elaborate or explain one's identifiability threshold. Further, concerning the format, it shall apply only to personal data processed by electronic means under the PDP Regulations.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Article 2 of the Electronic Information Law provides that it has an extraterritorial scope if the actions of individuals outside of Indonesia have a legal implication within the territory of Indonesia or if they adversely affect Indonesian interests. On a plain reading of the above provision, the Electronic Information Law may apply to breaches of personal data outside of Indonesia to the extent the effect concerns the personal data of Indonesian data subjects. However, we have not seen the government apply the PDP Regulations to entities outside of Indonesia.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The PDP Regulations define an ESP as a person, state administrator, business entity, or community that provides, manages, or operates an electronic system, individually or jointly, to or for electronic system users for their own or another party's benefit. The PDP Regulations do not recognise the concept of the processor. The PDP Regulations instead refer to an ESP as the party controlling and managing the use of personal data. Unlike controllers, the PDP Regulations do not refer to processors. Further, the PDP Regulations do not define data processors or distinguish them from data controllers. Therefore, we understand that the term 'data controllers' primarily refers to ESPs.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The PDP Regulations mandate the obtainment of consent for any processing of personal data. However, the PDP Regulations do not provide further guidance on how this consent is to be given.

In addition to consent, Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) stipulates lawful bases other than consent for processing personal data, which are:

- processing an individual's personal data to satisfy the obligations of a contract or to fulfil the request of such personal data owner when agreeing;
- the fulfilment of the legal obligation of the personal data controller in line with the applicable laws and regulations;
- guarding the vital interest of the personal data owner;
- performing the legal obligation of the personal data controller;
- performing the obligation of a public service personal data controller in the interest of the public; and
- satisfying another valid interest of the personal data controller or the personal data owner.

The wording in the relevant clause regarding lawful bases is rather ambiguous and may be interpreted to mean that consent is still required despite the existence of these lawful bases.

Further, under GR 71/2019, consent can only be considered lawful if it fulfils the following conditions:

- explicitly given, apparent and not hidden;
- shall not be based on fault, negligence or duress;
- for one or more specific purposes; and
- for the informed purposes.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Indonesia recognises that all information is personal data and shall receive the same processing and protection.

However, we understand that more stringent rules may apply in specific cases or circumstances (eg, in the financial services sector). Under OJK Circular Letter No. 14/SEOJK07/2014 on the Confidentiality and Security of the Personal Data or Information of Consumers, personal data consisting of name, address, birth date or age, phone number or the subject's biological mother's name can only be shared with a third party with the consent of the personal data owner or as is obligated by laws and regulations.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The PDP Regulations recognise the term transparency. For example, electronic system providers (ESPs) must notify data subjects of data breaches within 14 days of the discovery of a breach. In such regard, by nature, an ESP, acting as the controller of data, shall notify the individuals of the processing activities.

In particular for consent, although the PDP Regulations do not provide further guidance on how this consent is to be given, Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) and Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016) do provide more clarity on how the required consent is to be given.

MOCI Regulation 20/2016 defines 'consent' as:

> *a written manual or electronic statement given by a personal data owner after receiving complete disclosure of the acquisition, collection, processing, analysis, storage, display, announcement, transfer and disclosure, as well as the confidentiality or non-confidentiality, of the personal data.*

For consent, specifically, the following rules apply:

- consent must be obtained by any ESP that processes (including any acquisition and collection, processing and analysing, storage, repairs and updates, appearance, announcement, transfer, dissemination, disclosure or deletion or destruction) personal data;
- the consent may be given only after the owner of the personal data confirms the veracity, confidentiality or non-confidentiality, and purpose of the personal data; and
- the consent must be given in the Indonesian language, but there is no prohibition against the consent including a second language (eg, a bilingual Indonesian and English form).

In practice, ESPs will require consent to be both broad and as specific as possible, covering, among other things, transfer of the collected data to a foreign server via the internet and transfer of the collected data to a foreign server after the collected data has been stored in Indonesia if these actions are intended.

That being said, in practice, the notification usually covers the collected information, processing purposes and activities, lawful basis of processing activities, the possibility to share or transfer collected information, access to collected information, contact details of the ESP, and so on.

Exemptions from transparency obligations

15 | When is notice not required?

In general, the PDP Regulations do not provide conditions that may exempt ESPs from the notice requirement. In practice, it is uncommon for an ESP that acts as a service provider to notify the data subject after being contracted by the ESP that initially collected the data. By nature, such notifications may be considered to be given by the initial ESP through the notice of processing.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

MOCI Regulation 20/2016 provides that one of the key forms of personal data protection is that the processing of personal data must be under the original purpose of its processing. GR 71/2019 also provides that ESPs must disclose to the data subjects the purpose of their processing of the personal data. That being said, an ESP is obligated to maintain the accuracy of PI from collection to its deletion.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The PDP Regulations recognise the general restrictions for collecting PI: the PI collected must be relevant, in accordance with the purpose of the collection and implemented accurately. Although not yet been implemented, we note that the PDP Draft Bill recognises that PI that may be collected must be restricted and specific, legal, proper and transparent. The PDP Regulations and PDP Draft Bill do not provide details of the type of PI that must be restrictively collected.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Data stored within an electronic system may be destroyed only after:

- the lapse of the regulatory data retention period under MOCI Regulation 20/2016 or any other regulation issued by the relevant authority; or
- upon the request of the data subject, unless otherwise governed under laws and regulations.

MOCI Regulation 20/2016 provides that ESPs must retain personal data for a minimum of five years unless stipulated otherwise by sectoral regulations. Data may be retained beyond the five-year period if it is to be used following its initial purpose.

Consent is also required for the deletion of data (which is considered a part of data processing). In practice, the form of consent that data subjects are required to provide to ESPs is worded as broad as possible to cover all types of data processing.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

MOCI Regulation 20/2016 provides that ESPs may only use the personal data of data subjects following the needs of the data subjects. Further, ESPs shall also ensure that the processing of the personal data shall be in line with the specific purpose that has been consented to by the data subject. Further, MOCI Regulation 20/2016 provides that one of the key forms of personal data protection is that the processing of personal data must follow the original purpose of its processing. The current regulatory framework does not specifically regulate the application of this restriction, including with respect to circumstances where an organisation would like to use PI for a new purpose.

GR 71/2019 provides that ESPs must disclose the purpose of their processing of personal data to the data subjects, which in some jurisdictions is referred to as the 'finality principle'. Further, MOCI Regulation 20/2016 provides that one of the key forms of personal data protection

is that the processing of personal data must follow the original purpose of its processing.

The current regulatory framework does not specifically regulate some types of leniency in the form of compatible processing or purposes.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

There are no express rules for automated decision-making. However, according to the PDP Regulations, unless provided otherwise by the laws and regulations, the use of any information through electronic media that involves the personal data of a person must be made with the consent of the person concerned. Any person whose rights are infringed may claim damages under this law.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The PDP Regulations provide that electronic system providers (ESPs) must keep data secure. Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) affirms this obligation and further provides that ESPs must have security procedures and infrastructure in place to prevent disruptions, failures and damage within electronic systems. GR 71/2019 does not go into further detail as to the minimum measures required for such security procedures and infrastructure, and to date this has not been regulated.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

In general, the PDP Regulations do not obligate ESPs to notify either the Minister of Communication and Informatics (MOCI) of a data breach, except for 'serious data breaches caused by third parties', as provided by GR 71/2019. Neither GR 71/2019 nor the PDP Regulations provide further guidance on how the above phrase is defined. However, based on our informal discussions with officials from the MOCI, the MOCI expects to be notified of any data breach.

While there is no expressed definition of data breach, the PDP Regulations recognise data breach as a situation where an ESP fails to protect obtained data and the data is used without the consent of the owner. In this regard, in the event of a data breach, ESPs must notify data subjects within 14 days of the discovery of the breach. In such regard, by nature, an ESP, acting as the controller of data, must notify the individuals of the processing activities.

In addition to the above, for data breach notification, under article 28(c) of Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation No. 20/2016), an ESP is required to deliver written notification to personal data owners if there is a failure to protect the confidentiality of personal data within the electronic system managed by the ESP. This written notification must be made in line with the following terms:

- accompanied by the reason or cause for the failure to protect such confidentiality;
- can be done electronically if the personal data owner has consented to such method of notification during the obtainment and collection of his or her personal data;
- must be ensured to have been received by the personal data owner if such failure of confidentiality has the potential to cause damages to those involved; and
- the written notification must be delivered to the personal data owner at the latest 14 days since knowledge of such failure.

If an ESP does not adhere to the above terms it may be subject to sanctions under MOCI Regulation 20/2016. Further, failure to provide timely written notification gives affected personal data owners the opportunity to submit a complaint to the MOCI, irrespective of whether such failure has any potential to cause damages.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Pursuant to Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016), electronic system providers (ESPs) are required to have internal documentation for the purpose of personal data protection. This is basically internal rules or policies for the management of personal data, as a form of preventive measure against failures to protect the personal data the ESP manages. The PDP Regulations do not further elaborate on the forms of this internal documentation.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The PDP Regulations do not recognise the concept of a data protection officer. Therefore, appointing a data protection officer is not mandatory under Indonesian law. However, MOCI Regulation No.20/2016 requires that individuals be informed of the contact details of a designated contact person for enquiries into the data processing activity of an ESP. The PDP Regulations do not specifically regulate sanctions for failure to comply with this requirement. However, this may change shortly with the enactment of the Personal Data Protection Draft Bill.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

In general, an ESP is required to implement internal guidelines or policies for the collection, processing, and transfer of personal data and implement an audit record related to the provision of its electronic system. Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) also requires ESPs to record processing activities within their electronic systems, including personal data processing.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

While there are no specific rules for risk assessment in relation to certain uses of PI, pursuant to GR 71/2019, ESPs must apply risk management to prevent possible damage or loss, which includes conducting risk analysis and formulating mitigation measures and countermeasures to the threats within the electronic systems they manage, which may also contain PI.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

To the best of our knowledge, there is no obligation in relation to how PI processing systems must be designed. However, an ESP will be required to implement certain technical and organisational measures when processing personal data.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

To the best of our knowledge, PI owners or processors of PI are required to obtain a certificate of registration as an electronic system provider (ESP). Apart from registration as an ESP, we do not believe that there is presently any other obligation for owners or processors of PI to register with the Minister of Communication and Informatics (MOCI).

Other transparency duties

29 | Are there any other public transparency duties?

To the best of our knowledge, presently other than the obligation to register as an ESP, there is no other obligation for owners or processors of PI to register with the MOCI.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

To the best of our knowledge, there is no specific provision that governs outsourced processing services under the PDP Regulations. The current PDP Regulations do not differentiate between the data controller and data processor.

In this regard, there is a general requirement to obtain a legal ground for outsourcing processing services, as they constitute an act of processing. In practice, an electronic system provider (ESP) may include these outsourced processing activities in the notice or privacy policy (or consent request form, if using consent). Further, should the outsourced services involve transnational data transfers, certain requirements need to be complied with under Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016) by submitting a report of the cross-border transfer of personal data, both before and after conducting the transnational transfer. In practice, this report may be submitted annually to the MOCI.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Other than a general requirement requiring consent to collect personally identifiable information, to the best of our knowledge, there are no specific restrictions on the sharing of personal data within Indonesia, except for prohibited data including but not limited to that related to terrorism, child pornography or content that disturbs public order.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The PDP Regulations do not restrict international data transfers, except for by public scope ESPs. However, MOCI Regulation 20/2016 requires that the transfer of data overseas be done in coordination with the MOCI.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

In this regard, a general requirement shall apply equally to the transfers to service providers and onward transfers (both by the service providers or PI owners). This shall follow relevant provisions related to PI and the requirement to coordinate with the MOCI as regulated under MOCI Regulation 20/2016.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

If PI is contained in an electronic system or as data, then it is subject to the provisions on electronic systems and data protection under Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019). According to GR 71/2019, for public ESPs, PI should be retained in Indonesia. PI may be retained outside Indonesia only if the required technology or equipment is not available domestically. However, private ESPs may retain the PI in Indonesia and outside Indonesia. If the PI is retained outside Indonesia, private ESPs must ensure that the relevant Indonesian ministries and agencies are able to effectively monitor the overseas retention of such PI.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

The PDP Regulations provide that individuals as data subjects have the right to access their personal information held by PI owners. Other than the right to access, individuals as data subjects also have the rights as well as the limitation of rights as follows:

- the right of access to data or copies of data;
- the right to the rectification of errors;
- the right to the deletion or the right to be forgotten;
- the right to object to processing;
- the right to restrict processing;
- the right to data portability;
- the right to withdraw consent;

- the right to object to marketing; and
- the right to complain to the relevant data protection authority.

Other rights

36 | Do individuals have other substantive rights?

Other than the right of individuals to access their personal information, Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) acknowledges the right of delisting, which is the right of data subjects to have their personal data removed from search engines provided that the data is no longer 'relevant', based on a court order. The PDP Regulations do not elaborate on when personal data is considered 'irrelevant'. Nonetheless, we are of the view that the same rationale as to why data subjects may have their data erased if they withdraw consent should apply here.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016) acknowledges the right of data subjects to complain to the MOCI for the failure of an electronic system provider (ESP) to protect their personal data. Data subjects may submit a written complaint to the Directorate General of Application of Informatics (DGAI) within 30 business days from the discovery of the failure to protect the personal data of the data subject. If a violation is found, the DGAI may recommend that the MOCI impose certain administrative sanctions on the ESP. MOCI Regulation 20/2016 does not specifically mention the criteria for loss, but under the Indonesian Civil Code liability to compensate damages based on tort (an unlawful act) can be enforced if certain criteria are fulfilled – namely, an unlawful act and losses (ie, actual losses, damaged reputations or the PI owner has lost commercial opportunities), and there is a causal relationship between the unlawful act and the losses.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The MOCI or the DGAI, as the institution mandated by the MOCI to resolve such disputes, shall resolve the dispute through deliberation to reach a consensus or through any alternative mechanism. The official or institution in charge of settling such a dispute may provide a recommendation to the MOCI for the imposition of administrative sanctions on the breaching ESP. If the dispute resolution is ultimately unsuccessful the personal data owner and the other relevant ESPs may submit a civil claim against the ESP in breach.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

There are no derogations, exclusions, or limitations other than those already described, such as the requirement that the overseas transfer of data be done in coordination with the Minister of Communication and Informatics.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The PDP Regulations do not regulate the use of cookies.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

The PDP Regulations do not regulate this matter. However, we understand that more stringent rules may apply in specific cases, for example, in the financial services sector. Pursuant to Financial Services Authority (OJK) Regulation No. 1/POJK07/2013 regarding Financial Consumer Protection (6 August 2013), as last amended by OJK Regulation No. 18/POJK07/2018 (10 September 2018), a financial service provider is prohibited from disclosing customer data or information to third parties unless they receive written consent from the customer or are required to by law. If a financial service provider obtains the data or personal information of a person or a group of persons from a third party, it is required to obtain written confirmation from the third party that the person or group of persons has agreed to the disclosure. The above rules commonly apply to unsolicited ads or marketing communications by email, and telemarketing telephone calls or text messages.

We are not aware of any other rules pertaining to the sending of electronic direct marketing materials.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no express rules on targeted online advertising. However, according to the PDP Regulations, unless provided otherwise by the laws and regulations, use of any information through electronic media that involves the personal data of a person must be done with the consent of the person concerned. Any person whose rights are infringed may claim for damages under this law.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The PDP Regulations do not expressly recognise sensitive categories of personal information. However, for private electronic system providers, Minister of Communications and Informatics Regulation No. 5 of 2020 regarding Private Electronic Systems Providers (24 November 2020), as amended by Law No. 10 of 2021 (21 May 2021) recognises specific categories of PI, which consist of health data and information, biometric data, genetic data, sexual orientation, political views, data of children, personal financial data, and/or other data in accordance with the provisions of laws and regulations.

Profiling

44 | Are there any rules regarding individual profiling?

The PDP Regulations do not regulate this matter.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The PDP Regulations do not regulate this matter.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Indonesian House of Representatives (DPR) is in the process of finalising the Personal Data Protection Draft Bill (the PDP Draft Bill), which has been included by the DPR in the National Legislation Programme for 2022. The National Legislation Programme is a compilation of the top 50 draft bills that the DPR aims to ratify during the current five-year term of DPR members. However, despite being included in the National Legislation Program, there is no certainty as to when the PDP Draft Bill will be passed into law.

The current Draft Bill heavily resembles Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) of the European Union. In brief, the PDP Draft Bill is intended to clarify the scope of personal data, the roles and responsibilities of data controllers, data processors and data protection officers, and acknowledges most, if not all, of the rights of data subjects under the GDPR, and the general principles on consent to data processing.

Rusmaini Lenggogeni
rusmainilenggogeni@ssek.com

Charvia Tjhai
charviatjhai@ssek.com

14th Floor, Mayapada Tower I
Jl Jend Sudirman Kav 28
Jakarta 12920
Indonesia
Tel: +62 21 521 2038 / +62 21 2953 2000
Fax: +62 21 521 2039
www.ssek.com

Ireland

Shane Martin, Conor Daly and Coleen Wegmann
Walkers

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Since 25 May 2018, the key legislative instrument applicable in Ireland for the protection of PI has been the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). The Irish Data Protection Acts 1988 to 2018 (DPA) supplement and give further effect to the GDPR. Data protection is a fundamental right set out in article 8 of the EU Charter of Fundamental Rights and Irish courts have also recognised the right to privacy as one of the unenumerated rights recognised by the Irish constitution.

The legislative framework for the protection of PI also includes the Law Enforcement Directive (Directive (EU) 2016/680) in the context of criminal investigations and prosecutions. The Law Enforcement Directive is transposed into Irish law by the DPA.

The final key element of the legislative framework in Ireland is the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the Irish ePrivacy Regulations), which transpose the Privacy and Electronic Communications Directive 2002 (the ePrivacy Directive) into Irish law.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Data Protection Commission (DPC) is the independent data protection supervisory authority in Ireland with responsibility for the enforcement of the GDPR and safeguarding the fundamental right of individuals in the European Union to the protection of their PI. The DPC also has powers and responsibilities relating to the Irish ePrivacy Regulations and the Law Enforcement Directive.

The DPC's investigative powers include the power to:

- conduct investigations on compliance with the GDPR, including in the form of data protection audits and, where necessary, take enforcement action;
- investigate complaints received from individuals regarding potential infringements of data protection law;
- order individuals and organisations involved in the processing of PI to provide any information it requires for the performance of its tasks;
- carry out a review of data protection certifications issued by it pursuant to the GDPR;
- notify the controller or the processor of an alleged infringement of the GDPR; and
- obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with all applicable laws.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

As an EU data protection supervisory authority, the DPC is represented on the European Data Protection Board (EDPB). The EDPB works to ensure the consistent application of the GDPR across the European Union.

Under the GDPR, the DPC cooperates and collaborates with other data protection authorities on matters of legal interpretation and on specific cases through its participation in the 'one-stop-shop' mechanism. Under this mechanism, organisations that have their main establishment in an EU member state may elect to be primarily regulated by the supervisory authority of the jurisdiction in which their main establishment is located.

As part of the one-stop-shop mechanism, the DPC provides and receives mutual assistance to and from other concerned supervisory authorities and conducts joint investigations and joint enforcement actions with other concerned supervisory authorities.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

If the DPC finds that a breach of applicable data protection law has occurred, it may employ a number of different corrective powers. These corrective powers include facilitating amicable resolution of the matter, issuing a warning or reprimand to an organisation, issuing an order to bring data processing operations into compliance with the GDPR, imposing a temporary or permanent processing limitation on an organisation and imposing an administrative fine.

An administrative fine levied against an organisation for an infringement may be set at up to €20 million or 4 per cent of the organisation's total worldwide annual turnover for the preceding financial year (whichever figure is higher).

According to the GDPR, when deciding to impose an administrative fine on an organisation, the DPC must give due regard to a number of factors, including:

- the nature, gravity and duration of the infringement, as well as the number of individuals affected and the level of damage they have suffered;
- the intentional or negligent character of the infringement;

- any actions taken by the organisation to mitigate the damage;
- any previous infringements by the organisation;
- the categories of PI involved; and
- the manner in which the DPC has become aware of the infringement.

In addition to administrative sanctions, certain PI breaches can also lead to criminal sanctions. For example, the following breaches may constitute criminal offences:

- disclosure of a person's PI by a controller or processor, without prior authority;
- processing the PI of a child for the purposes of direct marketing, profiling or micro-targeting;
- obstructing an authorised officer of the DPC in the performance of his or her functions; and
- failing to comply with a requirement specified in a DPC enforcement notice.

Summary proceedings for an offence under the DPA may be brought and prosecuted by the DPC. Criminal penalties can include fines of up to €250,000, imprisonment for up to five years or both.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

PI owners have the right to appeal to the courts against orders of the DPC.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

While no particular sectors or types of organisation are exempt from the scope of the General Data Protection Regulation (GDPR) and the Irish Data Protection Acts 1988 to 2018 (DPA), some specific exemptions exist.

The GDPR states that the processing of PI by individuals for purely personal and domestic use are outside the scope of the GDPR.

The GDPR and the DPA also apply to public sector bodies. However, processing of PI by competent authorities for law enforcement purposes is outside the scope of the GDPR. Processing of PI for this purpose is subject to rules in Part 5 of the DPA.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Irish ePrivacy Regulations protect the confidentiality of electronic communications and also contain requirements relating to electronic marketing. Where electronic communications involve the processing of PI by organisations, the GDPR and the DPA will also apply.

The Postal Packets and Telecommunications (Regulation) Act 1993 provides a legislative basis for the lawful interception and covert surveillance in the context of the fight against organised crime and terrorism. The Irish government published proposals in 2020 to update the legislative framework in this area.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

There are a number of statutory instruments that provide specific data protection rules in the areas of health and social work, including:

- SI Number 18/2021 – Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2021;
- SI Number 82/1989 – Data Protection (Access Modification) (Health) Regulations 1989; and
- SI Number 83/1989 – Data Protection (Access Modification) (Social Work) Regulations 1989.

The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018, which implemented the EU Directive on the Security of Network and Information Systems, imposes information security standards and incident reporting-related obligations on digital service providers.

Outside the general principles provided for by the GDPR and the DPA, there is no specific legislation in Ireland governing the monitoring of employees. However, the right to privacy of a worker must be balanced against the right of an employer to protect its business interests. Any monitoring of employees by an employer in the workplace must be necessary, legitimate and proportionate, and such monitoring must be clearly communicated in the employer's privacy notice.

There is no specific legislation governing the use of social media by employees, however it is recommended that employers should have a clear policy on the acceptable use of social media in the workplace. Any monitoring of employees' social media use should be notified to employees and the purpose of such monitoring should be explained in the relevant policy or privacy notice. Profile screening of social media in recruitment and during employment can give rise to claims of discrimination and breach of privacy and data protection laws. Pre-hire criminal background checks are not permitted except where the role involves services being provided to children or vulnerable adults or work in the security industry.

PI formats

9 | What categories and types of PI are covered by the law?

The GDPR and the DPA apply to all forms of PI in electronic form and PI in manual form provided the latter forms part of, or is intended to form part of, a 'filing system'.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The GDPR applies to organisations established in any EU member state, including Ireland, where the organisation engages in the processing of PI of individuals. The GDPR will also apply to EU-based organisations where the processing of the PI takes place outside the European Union.

The GDPR also states that organisations established outside the European Union will be subject to the GDPR where they process the PI of individuals located in an EU member state (the targeted individuals) in connection with offering goods or services to such data subjects or in connection with monitoring the behaviour of such data subjects. Controllers or processors that come within the scope of the GDPR in this way must designate a representative in an EU member state where the targeted individuals are located.

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The GDPR contains a broad definition of processing such that virtually all processing and uses of PI by a controller or processor will be covered by the GDPR.

The GDPR identifies a controller as the party that, alone or jointly with others, determines the purposes and means of the processing of PI. The GDPR defines a processor as an individual or organisation that processes PI on behalf of a controller. The GDPR also notes that a processor must not process PI except on the instructions of the controller.

Both controllers and processors have certain duties and responsibilities in relation to the appropriate and secure processing of PI under the GDPR. However, the controller is the primary decision maker and has primary responsibility in relation to the PI.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The GDPR states that the processing of PI will only be lawful when one or more of the following lawful bases apply to the processing of the PI:

- the data subject has given prior, freely given and informed consent to the processing of his or her PI for one or more specific purposes. Importantly, consent should not be relied upon as a legal basis where there is a clear imbalance of power between the data subject and the controller;
- processing is necessary for the performance of a contract to which the data subject is party or 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 (not including contractual obligations or obligations arising under the law of a non-EU jurisdiction) to which the controller is subject;
- processing is necessary 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; and
- 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.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

The GDPR provides for a number of specific requirements for the lawful processing of sensitive PI (also known as 'special categories of PI'). The GDPR describes sensitive PI as including PI revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health; and
- data concerning a natural person's sex life or sexual orientation.

To lawfully process sensitive PI in accordance with the GDPR, the controller must establish that: (1) one of the lawful bases for processing non-sensitive PI applies to the processing of the PI; and (2) one of the additional grounds for processing sensitive PI as set out in the GDPR applies to the processing of the sensitive PI.

The additional grounds for the lawful processing of sensitive PI according to the GDPR include the following:

- the data subject has given prior explicit, freely given, informed consent to the processing of their sensitive PI for one or more specified purposes;
- processing is necessary in the context of employment and social security and social protection law;
- 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;
- 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 PI is not disclosed outside that body without the consent of the data subjects;
- processing relates to PI that is manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of EU or EU member state law; and
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EU or EU member state law.

The Irish Data Protection Acts 1988 to 2018 (the DPA) also include some additional grounds that may provide a legal basis for the processing of sensitive PI. These include processing sensitive PI for the following purposes as further defined in the DPA:

- employment and social welfare law;
- legal advice and legal proceedings;
- by the Irish Referendum Commission in connection with the electoral activities;
- the administration of justice;
- insurance and pension purposes;
- substantial public interest; and
- public health.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Pursuant to the General Data Protection Regulation (GDPR), controllers must adhere to the principle of transparency when processing PI and are required to provide certain information to the data subject at the time the PI is collected. To comply with these requirements, controllers typically provide data subjects with a data privacy notice containing the following mandatory information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the controller's data protection officer, where applicable;
- the purposes of the processing for which the PI are intended as well as the legal basis for the processing;
- the recipients or categories of recipients of the PI, if any;
- where applicable, the fact that the controller intends to transfer PI to a third country and details of the safeguarding mechanism to be relied upon to ensure the security of the PI being transferred;
- the period for which the PI will be stored;
- the existence of the right of the data subject to request from the controller access to and rectification or erasure of or restriction of processing of their PI or to object to the processing of their PI, as well as their right to data portability;
- where the legal basis for processing is the data subject's consent, the existence of the right to withdraw consent at any time;
- the right to lodge a complaint with the Data Protection Commission or another relevant EU data protection supervisory authority;
- whether the provision of PI is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the PI and of the possible consequences of failure to provide such data; and
- the existence of automated decision-making, including profiling, including the significance and the envisaged consequences of such processing for the data subject.

If the controller wishes to further process a data subject's PI for a new purpose after it has been collected, the controller must provide the data subject with information on that other purpose prior to that further processing.

Where PI has not been obtained directly from the data subject, the controller must provide the data subject with a privacy notice:

- within a reasonable period after obtaining the PI, but at the latest within one month;
- if the PI is to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- if the PI is to be disclosed to another party, the notice should be provided when the PI is first disclosed, at the latest.

Exemptions from transparency obligations

15 | When is notice not required?

It is not necessary to provide a privacy notice where:

- the data subject already has the information that would be included in the privacy notice;
- the provision of the privacy notice would be impossible or would involve a disproportionate effort (in such cases the controller must take appropriate measures to protect the data subject's rights and freedoms, including making the information publicly available);
- obtaining or disclosing the PI is expressly provided for under EU or EU member state law to which the controller is subject and that law provides appropriate measures to protect the data subject's legitimate interests; or
- where the PI is subject to an obligation of professional secrecy regulated by EU or EU member state law.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Controllers and processors engaging in the processing of PI must abide by the principles relating to the processing of PI. One of the principles relating to the processing of PI is that PI must be accurate and, where necessary, kept up to date.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Controllers and processors engaging in the processing of PI must comply with the data processing principle of ensuring the PI they process is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (known as the principle of data minimisation).

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Controllers and processors engaging in the processing of PI must comply with the principle of data minimisation.

PI must be held in a form that permits identification of data subjects only for as long as is necessary for the purposes for which the PI is processed (known as the principle of storage limitation).

There are no specific limits set out in the GDPR or the DPA to be complied with to satisfy the principles of data minimisation or storage limitation. However, time limits for the retention of records containing PI may be specified in other legislation such as anti-money laundering legislation.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The GDPR provides that PI may only be processed for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes. This principle is known as purpose limitation.

The processing of PI for purposes other than those for which the PI was initially collected is only permitted where the further processing is compatible with the purposes for which the PI was initially collected. In such a case, notice of the new purposes must be provided to the data subject. Where the new purposes would be incompatible with the original purposes, the consent of the data subject will be required unless an exemption applies.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

An individual has the right to not be subject to automated decisions without human intervention that affect them. Such automated decision-making is permitted only with the express consent of the individual, when necessary for the performance of a contract or when authorised by EU or member state law. Where one of these exceptions applies, suitable measures must be in place to safeguard the individual's rights, freedoms and legitimate interests. Where automated processing relates

to special categories of personal data, processing is only lawful where the individual has given express consent to the processing, or where it is necessary for reasons of substantial public interest.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The General Data Protection Regulation (GDPR) imposes a general obligation on owners of PI (controllers) and service providers that process PI on their behalf (processors) to ensure the security of data subjects' PI by implementing 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk'. The measures that an organisation chooses to implement must be assessed in the context of 'the nature, scope, context and purposes of processing' together with the risk and potential impact of a data security breach on the rights and freedoms of natural persons.

The GDPR provides examples of steps that controllers and processors may use to secure the PI for which they are responsible including:

- the pseudonymisation and encryption of PI; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

When appointing a processor, a controller must ensure that the contract appointing the processor requires the processor to employ all necessary security measures to ensure compliance with the GDPR.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Pursuant to the GDPR, controllers are required to notify the Data Protection Commission (DPC) of a data breach without undue delay, and no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

The GDPR also requires controllers to notify a data breach to the affected individuals without undue delay where the PI breach is likely to result in a high risk to the rights and freedoms of the affected individuals. In circumstances where a controller has not communicated a data breach to the affected individuals, the DPC may require the controller to notify the affected individuals based on its assessment of whether the data breach would be likely to result in a high risk.

Processors are required to notify the relevant controller of a data breach without undue delay.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The General Data Protection Regulation (GDPR) integrates accountability as a key principle that requires that owners of PI put in place appropriate technical and organisational measures to be able to demonstrate what they did and its effectiveness, when requested.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The appointment of a data protection officer (DPO) is required where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing sensitive PI or PI relating to criminal offences and convictions on a large scale.

Organisations may also elect to appoint a DPO voluntarily, although such an appointment will need to comply with the requirements of the General Data Protection Regulation (GDPR). The DPO's appointment is required to be notified to the DPC, and the DPC has issued guidance on the experience and qualifications that a DPO should have to undertake the role. The guidance confirms that a DPO's level of qualification and experience should be determined according to the personal data processing operations carried out, the complexity and scale of data processing, the sensitivity of the data processed and the protection required for the data being processed.

A DPO is required by the GDPR to:

- inform and advise the controller or the processor and its employees of their obligations pursuant to the GDPR and other requirements of EU or EU member state data protection law;
- monitor compliance with the GDPR and with the policies of the controller or processor in relation to the protection of PI, awareness-raising, staff training and audits;
- provide advice where requested as regards any data protection impact assessment (DPIA) undertaken and monitor the performance of the DPIA; and
- cooperate with the supervisory authority and act as the contact point for the supervisory authority on issues relating to processing.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Controllers and processors of PI are required to maintain internal written records of all processing activities for which they are responsible.

In particular, the GDPR stipulates that a controller should record:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the controller's DPO;
- the purposes of the particular processing activity;
- a description of the categories of data subjects and of the categories of PI that are processed;
- the categories of recipients to whom the PI have been or will be disclosed;
- details of any transfers of PI to a third country or an international organisation, including the suitable safeguards employed in respect of the transfers;
- the time limits for retention of the PI being processed; and
- a general description of the technical and organisation security measures implemented in respect of the PI.

The GDPR also states that a processor must maintain a record of all processing activities undertaken on behalf of a controller, including:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the DPO;
- the categories of processing carried out on behalf of each controller;
- where applicable, details of transfers of PI to a third country or an international organisation, including the suitable safeguards employed in respect of the transfers; and
- where possible, a general description of the technical and organisational security measures implemented in respect of PI.

The obligations relating to record-keeping do not apply in circumstances where an organisation employs fewer than 250 persons. However, this exemption does not apply where the processing is likely to result in a risk to the rights and freedoms of data subjects, processing is not occasional or the PI being processed includes sensitive PI.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The GDPR requires that a controller carry out an advance assessment of the impact of envisaged processing operations on the protection of PI (known as a data protection impact assessment (DPIA)) where processing includes the use of new technologies and is likely to result in a high risk to the rights and freedoms of natural persons.

In particular, the GDPR provides that a DPIA will be required in the case of:

- automated processing, including profiling;
- processing on a large scale of sensitive PI or PI relating to criminal offences and convictions on a large scale; and
- large scale systematic monitoring of a publicly accessible area.

Pursuant to the GDPR, the DPIA must at least contain:

- a systematic description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of PI and to demonstrate compliance with the GDPR.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The GPDR requires controllers to ensure 'data protection by design' and 'data protection by default'. Data protection by design means embedding data privacy features into the design of projects at an early stage. Data protection by default means that the user service settings must be automatically data protection-friendly, and that only data necessary for each specific processing purpose should be gathered.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no requirement for controllers or processors to register with the Data Protection Commission in relation to the data processing activities that they undertake.

Other transparency duties

29 | Are there any other public transparency duties?

A controller or processor that appoints a data protection officer (DPO) must publish the contact details of the DPO.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

When appointing a service provider to provide data processing services, a controller must only use a processor that provide sufficient guarantees to implement appropriate security measures to meet the requirements of the General Data Protection Regulation (GDPR) and ensure the protection of the rights of the data subjects.

Controllers are also required to put in place a written contract with a processor containing a number of provisions as set out in the GDPR that require the processor to:

- act only on the documented instructions from the controller;
- ensure that persons that will process PI are subject to an obligation to keep the PI confidential;
- take all security measures required by the GDPR;
- obtain prior specific or general written authorisation of the controller before appointing any sub-processors and ensure that sub-processors are subject to obligations equivalent to those imposed on the processor;
- assist the controller insofar as possible to comply with the controller's obligation to respond to data subjects' rights requests;
- assist the controller in ensuring compliance with its obligations regarding notification of PI breaches to the supervisory authority and data subjects (where necessary) and to carry out data protection impact assessments;
- at the choice of the controller, delete or return the PI to the controller after the end of the provision of services by the processor;
- make available to the controller all information necessary to demonstrate compliance with the foregoing obligations, and allow the controller to carry out an audit; and
- notify the controller immediately if any instruction received from the controller infringes the GDPR.

In June 2021, the European Commission published standard contractual clauses for use between controllers and processors, which are entirely optional.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The disclosure, knowingly or recklessly, of a person's PI by a processor, without the controller's prior authority is restricted under the Irish Data Protection Acts 1988 to 2018 and breaches of that restriction are subject to administrative or criminal sanctions, or both. In addition, a person who, without the prior authority of the controller or processor, obtains PI and discloses the PI to another person, commits a criminal offence. Similar offences also exist where a person sells, or offers to sell, PI that is obtained without the controller or processor's authority.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Pursuant to the GDPR, it is not permitted for PI to be transferred from within the European Economic Area (EEA) to a jurisdiction outside the EEA, unless a safeguarding mechanism is put in place, examples of which include the following.

- Adequacy decision: PI may be transferred to a jurisdiction in respect of which a finding of adequacy has been issued by the European Commission.
- Standard contractual clauses: PI may be transferred by a controller to another controller or processor pursuant to the European Commission's pre-approved standard contractual clauses. In In June 2021, the European Commission adopted updated standard contractual clauses (which have been drafted to reflect the requirements of the GDPR) to govern cross-border transfers of personal data outside the EEA and to replace the standard contractual clauses previously adopted by the European Commission. The updated standard contractual clauses entered into force on 27 June 2021, subject to an implementation period. Data transfer arrangements concluded before 27 September 2021 on the basis of the pre-existing standard contractual clauses shall be deemed to provide appropriate safeguards, within the meaning of the GDPR, until 27 December 2022 (provided the nature of the particular data transfer remains unchanged). The Court of Justice of the European Union (CJEU) in the *Schrems II* case upheld the continuing validity of standard contractual clauses. However, the CJEU also stated that controllers or processors, when acting as data exporters, should consider the particular data protection regime in the destination jurisdiction and put in place appropriate supplementary contractual measures to ensure that the transferred PI is protected. On 21 June 2021, the European Data Protection Board (EDPB) issued recommendations on measures that supplement data transfer mechanisms (the Recommendations). The Recommendations contain guidance on additional measures that may be implemented to ensure compliance with the requirements for data transfers, as set out in the GDPR. The EDPB's adoption of the Recommendations follows the CJEU's judgment in the *Schrems II* case.
- Binding corporate rules: PI may be transferred on the basis of intra-group binding corporate rules that have been approved by the DPC or another data protection supervisory authority in another EEA jurisdiction.

Following the UK's departure from the EU, transfers of PI can continue to flow freely without putting in place any additional safeguarding mechanism pursuant to the adjudication of the European Commission as to the adequacy of the UK's data protection regime.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions that apply under the GDPR to transfers from within the EEA to outside the EEA, apply equally to transfers to service providers (processors) and to any onwards transfers.

The CJEU's findings in the *Schrems II* case provide a clear reminder that the protection granted to PI in the EEA must travel with the PI wherever it is transferred. The transfer of PI to third countries cannot result in the protection afforded to PI in the EEA being undermined. As such, PI that is transferred to another controller or processor outside the EEA pursuant to one of the safeguarding mechanisms provided for under the GDPR must be afforded the same protection when being further transferred by the initial recipient.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no data localisation requirements in Ireland under applicable laws, including the GDPR and the DPA.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the General Data Protection Regulation (GDPR), data subjects have the right to obtain from the controller (1) confirmation as to whether or not their PI is being processed by the controller and (2) where their PI is being processed. They also have the right to the following information:

- the purposes of the processing;
- the categories of PI being processed;
- the recipients or categories of recipients with whom the PI may, or has, been shared;
- the safeguards put in place in respect of any international transfers of the PI;
- the retention period for the PI;
- the existence of the rights available to them under the GDPR, including the right to make a complaint to the Data Protection Commission (DPC) or other relevant data protection authority;
- where the PI was not collected from them directly, information as to the source of the data; and
- existence of any automated decision-making, details of and an explanation of the logic involved as well as the significance and the envisaged consequences of such processing for them.

In addition to the information listed above, controllers must provide data subjects with a copy of their PI, free of charge. Where the request is manifestly unfounded or excessive, the controller may charge a reasonable fee to cover administrative costs in complying with the request and may reject repeated identical requests.

Controllers must comply with the requirements set out above without undue delay and in any event within one month of receipt of the request (subject to extension in certain circumstances).

The Irish Data Protection Acts 1988 to 2018 (DPA) detail certain exceptions to a data subject's right of access. The restrictions on data subjects' access rights include where information is subject to legal

privilege, where the information comprises an opinion of a third party given in confidence or where PI is processed for the purpose of estimating the amount of the liability of the controller on foot of a claim. In addition, the right of access to PI must not adversely affect the rights of third parties.

Other rights

36 | Do individuals have other substantive rights?

Individuals have the following additional substantive rights:

- the right to the rectification of their PI that is inaccurate;
- the right to the erasure or deletion of their PI in certain circumstances, for example, when the PI is no longer necessary for the purposes for which it was collected by the data controller;
- the right to object to the processing of their PI;
- the right to receive a copy of their PI in a structured, commonly used and machine-readable format, and to transmit that PI to another controller without hindrance, to the extent that it is technically feasible;
- the right to have the processing of their PI restricted in certain circumstances; and
- the right not to be subject to a decision based solely on the automated processing of PI, including profiling, except in particular circumstances.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under the DPA, a data subject may receive compensation for any material and non-material damage suffered as a result of their data privacy rights under the GDPR or the DPA, or both, having been infringed.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

In circumstances where a data subject considers their data privacy rights under the GDPR or the DPA, or both, have been infringed, the data subject may bring a court action founded in tort against the controller or processor concerned. The Circuit Court, concurrently with the High Court, has jurisdiction to hear and determine such actions.

The DPC has no power to award compensation to affected individuals.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

The General Data Protection Regulation (GDPR) provides that each EU member state may restrict the scope of certain obligations and rights created under the GDPR. Accordingly, the Irish Data Protection Acts 1988 to 2018 include a number of exceptions to the rules that apply generally to the processing of PI including the following:

- that the processing of PI for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression, shall be exempt from compliance with the GDPR;
- an exception from the requirement that PI be processed only in accordance with the purpose for which it was collected in the case of issues relating to national security or prosecution of criminal offences;
- an exception from controllers' obligations and limitation of data subjects' rights for important objectives in the public interest (eg, safeguarding national security); and
- a limitation on the exercise of data subjects' rights in relation to archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The legal regime that currently applies to the use of cookies is the ePrivacy Directive 2002 and the Irish ePrivacy Regulations, which transpose the ePrivacy Directive 2002 into Irish law.

Additionally, where cookies contain identifiers that may be used to target a specific individual, or where information is derived from cookies and other tracking technologies that may be used to target or profile individuals, this will constitute PI and its processing is also subject to the General Data Protection Regulation (GDPR).

The Irish ePrivacy Regulations require website operators to obtain a website user's freely given, specific, informed and unambiguous consent to the setting of cookies on their device. The Data Protection Commission (DPC) noted in guidance issued in April 2020 that this is the same standard of consent as required by the GDPR and that consent is required for the setting of cookies whether the cookies contain PI or not.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Organisations that wish to market by email, fax, telephone or other electronic channels must comply with the provisions of the GDPR, the Irish Data Protection Acts 1988 to 2018 and the Irish ePrivacy Regulations.

Pursuant to the Irish ePrivacy Regulations, an individual must give his or her freely given, specific, informed and unambiguous consent (eg, by specifically opting in) to receive any electronic marketing communications. The individual being targeted by the marketing communication may withdraw his or her consent to the communications at any time and has the right under the GDPR to object to the communications. In accordance with the principles of GDPR, the organisation issuing the marketing material must make the targeted individual aware of this right.

The Irish ePrivacy Regulations allow for direct marketing to take place without explicit consent in certain specific circumstances in the context of a sale of a product or service.

Under the Irish ePrivacy Regulations, marketing calls to mobile phones are prohibited unless:

- the caller has been notified by the targeted individual that he or she consents to the receipt of such calls on his or her mobile telephone; or
- the targeted individual has consented generally to receiving marketing calls to his or her mobile phone and such consent to receive marketing calls is recorded in the national phone directory.

Targeted advertising

42 | Are there any rules on targeted online advertising?

Targeted online advertising often involves a number of separate parties, including the providers of the platform via which the targeted advertisement is delivered (the platform) and the individuals or companies that seek to use the platform to target or direct certain advertisements or messages at data subjects. Each of these parties must ensure that the personal data that is processed in connection with the tailoring of the advertisements and delivery of those advertisements is processed in accordance with the provisions of the GDPR. This will include establishing a legal basis for the processing of the targeted individuals' personal data and processing that personal data in accordance with the data processing principles set out in the GDPR. Of particular relevance in the context of targeted advertising will be ensuring compliance with the 'transparency principle' under the GDPR, which requires those controllers to provide the data subjects that receive the targeted advertisement with complete details of the means by which the targeted advertisement has been delivered.

Compliance with the GDPR in this context will also require the providers of a platform and the targeting entities to consider whether they are in fact 'joint controllers' for the purposes of the GDPR and, if so, what legal basis they have for processing the relevant data subjects' personal data.

Finally, prior to commencing online targeting operations, controllers should examine whether the processing operations are 'likely to result in a high risk' and, accordingly, conduct a data protection impact assessment (DPIA). If the social media provider processes 'special categories of data' under the GDPR, which includes 'special categories of personal data', it must find a legal basis for the processing in article 6 GDPR and rely on an exemption, such as explicit consent.

The European Data Protection Board published guidelines on 2 September 2020 that provide further information on the legal considerations arising in the context of targeted advertising.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Under the GDPR 'special categories of personal data' include data about an individual's health, racial or ethnic origin, biometry, religious or philosophical belief, political opinion, trade union membership, sex life or sexual orientation. Article 9 of the GDPR prohibits the processing of these special categories of personal data, except in certain excepted circumstances.

Circumstances where the processing of special categories of personal data is permitted under the GDPR include where the data subject has given explicit consent to the processing of the personal data and 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 and social security.

Based on the fact that the risks associated with processing special categories of personal data are higher, controllers and processors engaging in the processing of such personal data will be required to implement appropriate technical and organisational measures to ensure a level of security that is appropriate to that risk.

When processing special categories of personal data on a large scale, a controller is required to carry out a DPIA.

WALKERS

Shane Martin
shane.martin@walkersglobal.com

Conor Daly
conor.daly@walkersglobal.com

Coleen Wegmann
coleen.wegmann@walkersglobal.com

The Exchange
George's Dock
IFSC
Dublin 1
Ireland
Tel: +353 1 470 6600
Fax: +353 1 470 6601
www.walkersglobal.com

Profiling

44 | Are there any rules regarding individual profiling?

Article 22 of the GDPR states that a '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 him or her or similarly significantly affects him or her'.

There are exceptions to this prohibition on decision-making based on automated processing, including where a particular decision is necessary for entering into, or performance of, a contract between the data subject and a controller, where expressly permitted under EU or EU member state law, or where the processing is carried out based on the data subject's explicit consent.

Where a controller utilises automated processing, the controller should employ suitable safeguards, which should include specific information of the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The GDPR does not include any specific provisions relating to the use of cloud computing services or the outsourcing of activities by organisations to cloud service providers.

However, the DPC has issued guidance that details the security and transparency considerations that controllers should consider when using cloud computing services or engaging cloud service providers. These considerations are based on the principles for data processing set out in the GDPR.

The guidance emphasises the importance of putting in place a GDPR-compliant contract between the controller and the cloud computing service (which will typically be a processor) and ensuring that a safeguarding mechanism is implemented for any transfers of PI to a cloud computing service or cloud service provider located outside the European Economic Area.

Finally, entities that are regulated by the Central Bank of Ireland or an equivalent regulatory authority may be subject to an extra layer of regulation in relation to the use of cloud computing services or outsourced service providers.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Various multinational big tech organisations are headquartered in Ireland and, as such, the Data Protection Commission (DPC) plays a significant global role in regulating their activities as competent supervisory authority. This means Ireland has been at the centre of a number of recent developments in international data protection, including changes to the regulation of international data transfers and significant enforcement proceedings under the General Data Protection Regulation (GDPR). In the past year, the DPC has issued a number of significant enforcement decisions and fines.

The year 2021 also saw the introduction by the European Commission of the new standard contractual clauses governing transfers of personal data to countries outside the EEA. The new standard contractual clauses were also accompanied by the issuance of the European Data Protection Board recommendations on measures that supplement transfer mechanisms following the Court of Justice of the European Union's *Schrems II* decision in 2020. The European Commission also adopted standard contractual clauses for use by controllers when appointing processors to process data on their behalf.

In the past year, the DPC has also been active in publishing detailed guidance in a number of areas including in relation to a child-oriented approach to data processing.

Italy

Davide Baldini, Antonio Landi, Paolo Balboni, Luca Bolognini and Floriana Francesconi

ICT Legal Consulting

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The primary legislation governing the processing of personal data by private entities and public institutions in Italy is Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR). Specific rules for privacy in the electronic communications sector are contained within EU Directive 2002/58/EC (the ePrivacy Directive). Specific Italian legislation on data protection is outlined in Legislative Decree No. 196/2003 (the Personal Data Protection Code), which implements the ePrivacy Directive and has been largely amended by Legislative Decree No. 101/2018 to align its content with the GDPR.

EU Directive 2016/680 specifically regulates the processing of personal data by public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It has been implemented in Italy by Legislative Decree No. 51/2018.

Additional sector-specific guidance is set out in the supervisory authority's decisions, recommendations and guidelines (eg, as regards system administrators and the processing of personal data relating to fidelity cards).

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Italian Data Protection Authority oversees data protection legislation. Its investigative powers include the ability to obtain access to information – including personal data – from the data controller or processor and the power to carry out on-premise audits and inspections. When carrying out formal inspections, the Italian Data Protection Authority can demand copies of manual records and databases. The decisions of the Italian Data Protection Authority are published.

Data protection rules may also be enforced by judicial authorities when they hear claims brought by individuals.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Yes. On a general level, supervisory authorities are bound under article 61 of the GDPR to provide each other with relevant information and mutual assistance, with particular regard to information requests and supervisory measures, such as the carrying out of authorisations and consultations, inspections and investigations.

Moreover, article 60 of the GDPR envisages provisions on cooperation between supervisory authorities in the cases of cross-border processing between EU member states. In this latter case, articles 56(1) and 56(2) identify, respectively, the lead supervisory authority and one or more concerned supervisory authorities. The lead authority has primary responsibility for dealing with the cross-border data processing activity, while concerned authorities must be involved in the decision to express their views on the matter. In a cross-border processing scenario, all authorities involved are legally obliged to exchange all relevant information with each other, while the lead authority must submit a draft decision to the concerned authorities to take due account of their views.

When the lead and concerned authorities are unable to reach a common decision, or where there is no agreement on which supervisory authority is the lead authority, article 63 and onwards of the GDPR envisages a consistency mechanism whereby the European Data Protection Board has the final word on the matter by issuing of a binding decision.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Yes. Breaches of the GDPR and the Personal Data Protection Code are subject to the administrative sanctions provided under article 83 of the GDPR, which can be as much as €20 million or, for undertakings, up to 4 per cent of total worldwide annual turnover, if higher. Moreover, under article 58 of the GDPR, the supervisory authority may impose a temporary or definitive limitation including a ban on processing.

Under EU law, the provision of criminal penalties is generally determined by EU member states. In Italy, the Personal Data Protection Code includes several criminal provisions relating to certain instances of wilful unlawful processing of personal data and the wilful provision of false information to the supervisory authority. Only natural persons may incur a criminal sanction, while both natural and legal persons may incur an administrative sanction.

Administrative sanctions may be imposed by the supervisory authority; criminal penalties may be issued only by the judicial authority.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Yes, data controllers, data processors and data subjects alike can file appeals against orders of the Italian Data Protection Authority. According to article 152 of the Personal Data Protection Code, all disputes concerning the matters covered by the judicial remedies referred to in articles 78 and 79 of the GDPR and those concerning the application of the legislation on the protection of personal data, as well as the right to compensation for damage pursuant to article 82 of the GDPR, fall within the competence of the ordinary judicial authority.

In particular, the ordinary judicial authority has jurisdiction over appeals brought against the decisions issued by the data protection authority.

The decision of the court is not subject to appeal; the only remedy available is, according to the ordinary procedural rules, the possibility to lodge a judicial redress to the Supreme Court to assert violations of the law.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR) applies to both private and public organisations when they process personal data, even when public organisations perform activities in the public interest.

However, the GDPR does not apply to some instances of personal data processing, as provided by article 2(2):

- in the course of an activity that falls outside the scope of EU law;
- by the EU member states when carrying out activities that fall within the scope of Chapter 2 of Title 5 of the Treaty on European Union, which regulates EU competence in matters of foreign and security policy; and
- by a natural person in the course of a purely personal or household activity (in paragraph 30 of case C-212/13, the Court of Justice of the European Union held that this exemption should be interpreted narrowly).

Legislative Decree No. 51/2018, which implements EU Directive 2016/680, specifically regulates the processing of personal data by public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Yes. Legislative Decree No. 51/2018, which implements EU Directive 2016/680, specifically regulates the processing of personal data by public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

More specifically, interception of communications is typically regulated by the Criminal Code and the Code of Criminal Procedure (article 266 and onwards), as amended by Legislative Decree No. 216/2017 and Legislative Decree No. 161/2019.

Where the monitoring and surveillance of individuals are carried out by private entities or by public authorities outside the purposes of Legislative Decree No. 51/2018, the GDPR and the Personal Data Protection Code apply.

Electronic marketing is regulated by the Personal Data Protection Code, that in part transposes the EU Directive 2002/58/EC (the ePrivacy Directive), and by the relevant decisions and guidelines of the Italian Data Protection Authority.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Being an omnibus regime, EU and Italian data protection law is not sector-specific and, as such, generally applies to all areas where the processing of personal data takes place.

More sector-specific guidance is typically outlined in the Italian Data Protection Authority's decisions, recommendations and guidelines, some of which were adopted before the GDPR became applicable but are still in force (eg, regarding system administrators, the processing of personal data relating to fidelity cards and social media marketing). Regarding e-health records, the Agency for Digital Italy has the relevant legislation published on its website.

PI formats

9 | What categories and types of PI are covered by the law?

Article 2(1) of the GDPR covers the processing of personal data wholly or partly by automated means (eg, data processed using a computer or any other electronic device) and processing other than by automated means of personal data that forms or is intended to form part of a filing system (eg, a paper-based archive).

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

As provided by article 4(2) of the GDPR, EU and Italian data protection law may apply to the processing of personal data that concerns natural persons who are in Italy but performed by entities not established in Italy, where the processing activities are related to:

- the offering of goods or services (even free of charge) to such natural persons in Italy; or
- the monitoring of their behaviour, as far as their behaviour takes place within Italian territory.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

EU and Italian data protection law applies to any operations that are performed on personal data.

The law distinguishes the data controller (ie, the entity that determines the purposes and means of the personal data processing (article 4(7) of the GDPR)) and the data processor (ie, the entity that processes the personal data on behalf of the data controller (article 4(8) of the GDPR)).

The law provides for different duties for data controllers and processors, although some obligations apply to both (notably, security obligations under article 32 of the GDPR).

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes. Any processing of personal data must be grounded on one or more of the six legal bases provided by article 6(1) of Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR). In particular, any processing of personal data is lawful when the data subject has provided their consent or where the processing is necessary:

- for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;
- for compliance with a legal obligation to which the data controller is subject;
- to protect the vital interests of the data subject or another natural person;
- for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; or
- 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.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Yes. The processing of certain categories of personal data that pertains to intimate aspects (eg, genetic data and data concerning health, or revealing racial or ethnic origin – special categories of personal data) is generally prohibited under article 9(1) of the GDPR. The processing of such data shall be grounded on one of the narrow exceptions set forth by article 9(2) of the GDPR, provided that one of the legal bases set forth by article 6(1) of the GDPR also applies.

Similarly, the processing of personal data relating to criminal convictions and offences must be based on one of the legal bases provided by article 6(1) and carried out under the control of the official authority or when the processing is authorised by law.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Yes. Under article 13 of Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR), where personal data is collected directly from the individual, the data controller must provide the following information:

- the identity and contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where present;
- the purposes of the processing for which the personal data is intended and the relevant legal basis;
- where the processing is based on the legitimate interest ground, which legitimate interests are being pursued;
- the recipients or categories of recipients of the personal data, if any;
- whether the controller intends to transfer personal data to a third country or international organisation, along with further information regarding the lawfulness of the transfer;
- the period for which the personal data will be stored or, if that is not possible, the criteria to determine that period;
- the existence of each data subject's rights;
- where the processing is based on the data subject's consent, the existence of the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- the existence of automated decision making, including profiling, which produces legal effects or similarly significantly affects the data subject, and meaningful information about the logic involved, as well as the significance and possible consequences of such processing for the data subject.

Where personal data is not collected from the data subject, under article 14 of the GDPR, the data controller shall provide the data subject with the same information set forth by article 13, in addition to the categories of personal data concerned, the source from which the personal data originates and whether it came from a publicly accessible source.

This information must be provided before the processing.

Exemptions from transparency obligations

15 | When is notice not required?

Under articles 13(4) and 14(5)(a) of the GDPR, the provision of information to the data subject is not required insofar as the data subject already has the information.

Moreover, where personal data is not collected from the data subject, under articles 14(5)(b) to (d) of the GDPR, the provision of information is not required in the cases where, respectively:

- provision proves impossible or would involve a disproportionate effort;
- obtaining or disclosure is expressly laid down by EU or EU member state law to which the controller is subject; or
- the personal data shall remain confidential subject to an obligation of professional secrecy.

National provisions on personal data processing activities in the context of the covid-19 pandemic need to be constantly checked to be aware of relevant notification exceptions.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes. Under article 5(1)(d) of the GDPR, personal data must be accurate and, where necessary, kept up to date.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Yes. According to the minimisation principle, pursuant to article 5(1)(c) of the GDPR, data controllers must only collect and process personal data

that is relevant, necessary and adequate to accomplish the purposes for which they are processed. The practical implementation of this principle requires applying two concepts to the personal data processing purpose pursued by the data controller: necessity and proportionality. 'Necessity' entails that all categories of personal data processed are genuinely needed to successfully pursue the stated purpose of the processing, while 'proportionality' requires that the categories of personal data processed are not excessive in relation to the stated purpose of the processing.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Yes. The law restricts both the amount of personal data and the length of time for which it may be held.

As regards the amount, according to the minimisation principle, pursuant to article 5(1)(c) of the GDPR, data controllers must only collect and process personal data that is relevant, necessary and adequate to accomplish the purposes for which it is processed.

Concerning the length of time, according to the storage limitation principle laid down by article 5(1)(e) of the GDPR, personal data must be:

> *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes . . .*

In other words, personal data must not be kept for longer than necessary for the purposes for which they are processed and, once the information is no longer needed, personal data must be securely deleted. To ensure that the personal data is not kept longer than necessary, time limits should be established by the data controller for erasure, anonymisation or a periodic review. In practice, thus, the data controller must determine the period of personal data retention in line with the above principle and taking into account the purposes for which the data is processed.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

In principle, the controller may process the personal data for any purpose, as long as it is legitimate.

The GDPR has adopted the principle of purpose limitation in article 5(1)(b), pursuant to which personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Article 6(4) of the GDPR envisages a general test of compatibility between the original and the new purpose, under which the latter is allowed where the controller has successfully carried out and documented the outcome of such test.

Processing for new purposes is also allowed where the data subject has provided their consent or where the processing is based on the law.

Moreover, under article 6(1)(d), processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not to be considered incompatible with the initial purposes, where it respects article 89(1).

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Yes. Article 22(1) of the GDPR establishes a general prohibition for decision-making based solely on automated processing, which, according to the Article 29 Working Party's Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, applies irrespective of the data subject's actions. The prohibition of subjecting a natural person to automated decision-making applies only if such a decision is based solely on automated processing and produces legal effects concerning the data subject or similarly significantly affects them. However, if an automated decision-making process falls within these parameters, the activity is allowed if it is authorised by European Union or member state law; necessary for entering into, or the performance of, a contract; or pursuant to the data subject's explicit consent, provided that the controller has put sufficient safeguards in place.

In cases where the decision is based on the special categories of personal data referred to in article 9(1) GDPR, the activity is lawful only where it is based on article 9(2) GDPR, letter (a) or (c) (ie, respectively, where the data subject has provided his or her explicit consent, or where processing is necessary for reasons of substantial public interest, on the basis of EU or member state law). In both cases, suitable measures to safeguard the data subject's rights, freedoms and legitimate interests must be put in place.

Without prejudice to the above, where the activity is based on the contract or on the data subject's explicit consent, the data controller also needs to '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 his or her point of view and to contest the decision'. While the suitable measures must be assessed and adopted by the data controller on a case-by-case basis, possibly within the context of the data protection impact assessment pursuant to article 35 GDPR, some possible measures are further elaborated on within Recital 71 GDPR, thereby including appropriate mathematical or statistical procedures and implementing appropriate technical and organisational measures to ensure, in particular, that factors that result in inaccuracies in personal data are corrected and the risk of errors is minimised, with a view of preventing, inter alia, discriminatory effects.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Both controllers and processors are accountable for the security measures they have implemented. Article 32 of Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR) requires the adoption of appropriate security measures – both technical and organisational – by taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons.

In 2018, the EU Agency for Network and Information Security issued the Handbook on Security of Personal Data Processing, which provides guidance on the minimum technical standards to be provided by companies for personal data processing and Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, which aim to provide a common approach at the EU level regarding security measures to be implemented by digital service providers.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Yes. In case of a data breach, the controller must, without undue delay and, where feasible, no later than 72 hours after having become aware of the breach, notify the supervisory authority. The data controller must provide to the authority the information outlined in article 33(3) of the GDPR, which includes:

- the nature of the personal data breach;
- the categories and approximate number of data subjects concerned;
- the likely consequences of the breach; and
- the measures taken or proposed to be taken to address it and mitigate its effects.

The supervisory authority need not be informed of the breach where it is unlikely to result in a risk to the rights and freedoms of data subjects, while both the authority and affected individuals must be informed where the breach is likely to result in a high risk for the persons concerned, under article 34 of the GDPR.

EU supervisory authorities have provided guidance on data breaches in their relevant guidelines. The Italian Data Protection Authority has made a template available for the notification of data breaches.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Yes. Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR) has formally embedded the requirement of accountability into the data protection legislative framework. It describes and extends the overall accountability of organisations that process personal data. In practice, the principle of accountability entails that the data controller must be able to provide evidence of their compliance with the obligations stemming from the data protection framework.

In particular, the principle of accountability is first introduced in article 5 of the GDPR. Article 5(1) lists the six fundamental principles relating to the processing of personal data (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality), and article 5(2) GDPR specifies that the data controller is responsible to both comply and be able to demonstrate compliance with the six principles outlined in article 5(1) GDPR.

Article 24 GDPR further specifies the accountability obligation and requires data controllers to implement appropriate technical and organisational measures, thereby including data protection policies, if appropriate, to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; furthermore, it requires the controller to regularly review and update those measures where necessary. Those measures should take into account the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of the individuals. If the relevant processing results in a higher level of risk to the rights of the individual, the data controller is required to adopt greater measures to protect against that risk.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Yes. The appointment of a data protection officer (DPO) is mandatory under specific circumstances. Under article 37 of the GDPR, as interpreted by the European Union supervisory authorities' relevant Guidelines on Data Protection Officers, organisations must appoint a DPO where their core activities consist of processing operations that require regular, systematic and large-scale monitoring of data subjects, or the large-scale processing of special categories of data or data relating to criminal convictions and offences.

According to paragraph 2 of the Guidelines, unless it is obvious that an organisation is not required to designate a DPO, data controllers and processors should document and update over time the internal analysis carried out to determine whether a DPO is to be appointed.

Under article 39, the DPO has the following tasks, which must be performed with due regard to the risk associated with the relevant processing operations:

- inform and advise the controller or the processor and the employees of their obligations under data protection law;
- monitor compliance with data protection law and with the policies of the controller or processor concerning personal data protection, including the assignment of responsibilities, awareness-raising, training and audits;
- provide advice where requested regarding the data protection impact assessment and monitor its performance; and
- cooperate with and act as the contact point for supervisory authorities.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Yes. Under article 30 of the GDPR, both controllers and processors (and, where applicable, their representatives) must maintain a record of processing activities. As also specified by the Italian Data Protection Authority within its FAQs published on 8 October 2018, this obligation does not apply where the organisation employs fewer than 250 persons, unless the processing it carries out is likely to result in a risk to data subjects, is not occasional, or includes special categories of data (eg, biometric data, genetic data, data concerning health, religious beliefs and ethnic origin, etc), or data relating to criminal convictions and offences. Such exceptions are to be interpreted in a restrictive way, based on the article 29 Working Party Position Paper related to article 30(5) of the GDPR on the derogations from the obligation to maintain records of processing activities under article 30(5) of the GDPR.

The obligation to maintain the record of the processing activities is one of the main elements of accountability for the data controller as it is a suitable tool to provide an updated picture of the processing activities carried out within the organisation, fundamental to conduct the risk analysis.

The record of processing activities must be in written and electronic form, and must be produced at the request of the Italian Data Protection Authority.

The Italian Data Protection Authority's FAQs indicate, among others, what information the record of processing activities should contain and how the record should be maintained and updated.

Moreover, under article 24(2) of the GDPR, where proportionate concerning their activities, controllers must implement appropriate data protection policies.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Yes. Article 32 of the GDPR incorporates a risk-based approach to data security, meaning that controllers and processors are required to carry out risk assessments when implementing new data processing activities to be able to establish and document security measures that are adequate for the activity performed, to protect the rights and freedoms of the data subjects. The requirement to carry out risk assessments is reinforced by articles 25 GDPR, which requires the data controller to implement data protection by design and by default principles in light of the relevant risks of the processing regarding the rights and freedoms of data subjects, and 35 GDPR, which requires the data controller to perform a full-fledged data protection impact assessment where the risk to the rights and freedoms of data subjects is deemed to be high.

These risk assessments must take into account, inter alia, the nature of the data that is to be processed and any reasonably foreseeable threat that will exploit business processes and technical system vulnerabilities. The risk assessments must also include a state-of-the-art test and a requirement to consider cost. The test has the effect of requiring controllers and processors to consider industry best practices and not simply common industry practices.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Yes. Article 25 of the GDPR envisages data protection by design and by default obligations towards data controllers.

Under article 25(1) of the GDPR, the controller must, before the processing, implement appropriate technical and organisational measures designed to implement data protection principles effectively and to integrate the necessary safeguards into the processing, to meet GDPR requirements.

Moreover, article 25(2) of the GDPR mandates the controller to implement appropriate technical and organisational measures to ensure that only personal data necessary for each specific purpose of the processing is processed by default.

Finally, the controller must perform a risk assessment on data subjects' rights before any new processing activity, to determine both the security measures to be implemented and the need to carry out a full data protection impact assessment on the processing.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

No.

Other transparency duties

29 | Are there any other public transparency duties?

Not applicable.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Before engaging an entity that processes personal data on its behalf (ie, a data processor), under article 28(1) of Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR), the data controller must ensure that the processor provides sufficient guarantees of compliance with the law. Moreover, under article 28(3), the processing of personal data between a data controller and a data processor must be regulated by a contract or other legal act that is binding on the processor and contains the minimum content required under such provision.

Conversely, the disclosure of personal data from a data controller to another data controller amounts to the processing of personal data and therefore requires the occurrence of a legal basis among those provided under article 6(1) of the GDPR.

Data subjects shall be informed beforehand of the possible disclosure of their personal data to a recipient or category of recipients, under articles 13(1)(e) and 14(1)(e) of the GDPR.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

There are no specific restrictions.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Personal data flows freely within the European Economic Area and countries that ensure an adequate level of protection under an adequacy decision adopted by the European Commission based on article 45 of the GDPR.

The European Commission's adequacy decisions, adopted under article 45 of the GDPR, are available online.

Other notable legal grounds in addition to the adequacy decisions for the transfer of personal data outside the European Economic Area include:

- standard data protection clauses approved by the European Commission: these contracts offer the additional adequate safeguards concerning data protection that are needed in the case of a transfer of personal data to any third country. The latest set of standard data protection clauses has been adopted with Commission Implementing Decision (EU) 2021/914 of 4 June 2021;
- codes of conduct and certification mechanisms: codes of conduct or a certification mechanism can offer appropriate safeguards for transfers of personal data if they contain binding and enforceable commitments by the organisation in the third country for the benefit of the individuals; and
- binding corporate rules: these are personal data protection policies adhered to by a group of undertakings to provide appropriate safeguards for transfers of personal data within the group, including outside of the European Economic Area.

Concerning the transfer of personal data outside the European Economic Area, on 16 July 2020, in its landmark judgment in *Schrems II* (case C-311/18), the Court of Justice of the European Union invalidated the adequacy decision on the EU-US Privacy Shield due to US domestic law requirements concerning surveillance. The Court found that storage and access for national security purposes to EU personal data that is transferred to the United States limits the level of protection afforded to

EU data subjects, leading it to conclude that the level of protection in the United States cannot be considered essentially equivalent to that found in the European Union and that the guarantees in place for non-US persons were inadequate.

In its decision, the Court also pointed out that Commission Decision 2010/87/EU that sets out the controller to third-country processor standard data protection clauses imposes an obligation on the data exporter and the recipient of the data (the data importer) to verify, before any transfer, whether the level of protection granted under EU law is met in the third country, taking into account the circumstances of the transfer and any additional guarantees that the data exporter may impose upon the data importer. The Court further noted that Commission Decision 2010/87/EU decision requires that the data importer informs the data exporter of any inability to comply with the standard data protection clauses due to conflicting obligations under local law, the latter then being, in turn, obliged to suspend the transfer of data or to terminate the contract with the former.

To help public and private organisations comply with the *Schrems II* judgment, on 10 November 2020, the European Data Protection Board issued 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data', which provides a six-point methodology to address data transfers and 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures', which summarise the requirements set forth by EU law for public surveillance measures to be lawful. The former document has undergone public consultation and is currently pending final approval by the EDPB. The six-step methodology addressing data transfer is as follows:

- the data exporter should map all transfers of personal data to third countries and verify that the transfer is adequate, relevant and limited to what is necessary concerning the relevant purposes;
- the data exporter should verify the safeguards for each transfer, among those listed under article 44 and following the GDPR;
- where the third country has not received an adequacy decision from the European Commission, the data exporter needs to assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the transfer tools that the data exporter is relying on, in the context of the specific transfer. This assessment should be carried out using the 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' as a benchmark, should be performed with due diligence, and must be thoroughly documented;
- if the third-country law or practice impinges upon the effectiveness of the relevant transfer tools, the data exporter, where appropriate in collaboration with the data importer, should adopt supplementary measures that are necessary to bring the level of protection of the data transferred in line with the European Essential Guarantees;
- the data exporter may need to take any formal procedural steps the adoption of the supplementary measures may require, depending on the transfer tools that the data exporter is relying on. Recommendations 01/2020 specify these formalities (eg, consultation of the competent supervisory authority); and
- under the principle of accountability, the data exporter should re-evaluate the level of protection afforded to the data transferred to third countries at appropriate intervals and monitor if there have been or will be any developments that may affect it.

Personal data may also be occasionally transferred in the exceptional circumstances provided for by article 49 of the GDPR, as interpreted by the relevant EU supervisory authorities' guidelines.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Restrictions on personal data transfers outside the European Economic Area also apply to onward transfers from the third country or international organisation to another third country or international organisation, under article 44 of the GDPR.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No. The GDPR and Italian data protection law do not require that a copy of personal data be retained within the Italian jurisdiction. Moreover, article 1(3) of the GDPR expressly prevents Italian law from establishing any restriction for the transfer of personal data to other countries within the European Economic Area.

On the other hand, articles 44–50 of the GDPR provide for specific requirements and limitations for the transfer of personal data to third parties located outside of the European Economic Area.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes. The right of access to personal data is provided under article 15 of Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR).

This right may be exercised by the data subject by any means (eg, by contacting the data controller via email or fax). However, the data controller, where possible, should provide remote access to a secure system that provides the data subject with direct access to the personal data (Recital 63).

Under article 12(5) of the GDPR, where requests from a data subject are manifestly unfounded or excessive, the controller may refuse to act on the request.

The possibility and conditions for EU or EU member state law to provide for limited and sector-specific restrictions to this and other rights are outlined in article 23 of the GDPR, subject to EU fundamental rights law requirements.

Other rights

36 | Do individuals have other substantive rights?

Yes. Data subjects have the following rights under the GDPR:

- the right to obtain from the controller the rectification of inaccurate or incomplete personal data under article 16;
- the right to obtain the erasure of their personal data in the cases provided under article 17; and
- the right to obtain the restriction of processing in the cases provided under article 18.

Article 20 gives data subjects the right to obtain their personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit such data to another controller, where the legal basis for the processing is the data subjects' consent or the performance of a contract.

Under article 21, where the processing is based on legitimate interest or the performance of a task carried out in the public interest or the exercise of official authority, the data subject has the right to object to the processing.

Finally, article 22 provides individuals with the prima facie right not to be subject to a decision based solely on automated decision making that produces legal effects or similarly significantly affects the individual.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes. Data subjects have the right to obtain compensation for both material and non-material damages suffered as a result of a breach of the GDPR, under article 82. Under Italian tort law, the plaintiff must be able to show both a breach of the law and the actual occurrence of (even non-material) damage.

Both the controller and processor are jointly and severally liable toward the data subject. The entity that has paid full compensation is entitled to claim back from the other entity involved in the same processing part of the compensation corresponding to their responsibility.

While the controller is liable for the damage caused by any processing that infringes the GDPR, the processor is liable only where it has infringed specific GDPR provisions addressed to processors or where it has acted contrary to or outside the legitimate instructions of the controller.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Data subjects' rights provided under articles 15 to 22 of the GDPR may be enforced by both the supervisory authority and the national courts.

The right to compensation for damages suffered as a result of the processing may be enforced only by bringing proceedings before the competent national court.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

No.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Article 122 of the Personal Data Protection Code (implementing the EU Directive 2002/58/EC (the ePrivacy Directive)) prescribes that the use of cookies or similar technologies that involve the storing of and accessing information that is already stored on a user's (either a natural or legal person) device are permitted, provided that the user has given their prior informed consent.

Technical cookies are exempt from this requirement. Technical cookies are used only to transmit a communication over an electronic communications network or for a service provider to deliver a service that has been explicitly requested by the user. Technical cookies may be used without the user's consent, provided that the user is informed thereof.

In 2021, the Italian Data Protection Authority issued guidelines on the use of cookies and other tracking technologies, which became applicable on January 2022. The guidelines stipulate that cookies used to measure traffic on a website (analytics cookies) are subject to the same rules governing technical cookies, provided that appropriate technical measures to reduce their power to identify a natural person are adopted and – in case of third-party cookies – an agreement is in place with the cookie provider that prohibits them from further processing the information gathered by the cookie.

For cookies and other tracking technologies used for profiling and marketing activities (profiling cookies), the Italian Data Protection Authority requires that their use is always subject to the prior consent of the user, with the same validity requirements set forth by the Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR). Such consent should be acquired, typically, by the publisher by means of a cookie banner with the following requirements:

- a command (eg, an 'X' placed on the top right corner) to close the banner without giving consent to the use of cookies or other profiling techniques and to keep default settings;
- a command (button) to accept all cookies or tracking tools; and
- a link to an additional dedicated area where the user can select, individually, the functionalities, third parties and cookies he or she consents to install, and where the user can either consent to the use of all cookies (if such consent has not already been given) or withdraw his or her consent, also once and for all. This dedicated area must be accessible through an additional link to be placed in the footer of each domain page.

The guidelines contain, moreover, some indications on passive tracking systems (such as fingerprinting), scrolling (which may amount to a valid means of obtaining a user's consent, if certain conditions are met), the tracking of authenticated users, the reiteration of user consent requests and third-party cookies.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

As a rule, paragraphs 1 and 2 of article 130 of the Personal Data Protection Code (implementing the EU e-Privacy Directive 2002/58/EC) prescribe that marketing communications carried out by means of email, fax, telephone and similar media require prior consent from the user (either a natural or legal person).

However, paragraph 4 of article 130 sets forth an exception to this rule: where the controller has processed the data subject's email address in the context of the sale of a product or service, the controller may send marketing communications to that email address, insofar as the data subject has been duly informed and has not objected to this processing.

With specific regard to telephone marketing activities, paragraph 3-bis of article 130 provides that data controllers may lawfully contact all the users that have not objected to receiving marketing communications by telephone, by enrolling in the Register of Oppositions. As regards the functioning of the register, Law 5/2018 provides that any user who enrols in the register withdraws any previously given consent to marketing by means of telephone, so that they may not be lawfully contacted for marketing purposes carried out through such means by any data controller. Moreover, article 1(12) of the law provides that a controller wishing to carry out marketing activities by telephone has a duty to consult the register at least monthly and, in any case, before the start of marketing campaigns.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules. In any case, considering that targeted advertising is usually performed by means of tracking and subsequent profiling of users' online behaviour across one or more websites and applications, this matter is mostly regulated by means of the rules governing cookies and similar technologies (ie, by article 122 of the Personal Data Protection Code (transposing the EU e-Privacy Directive 2002/58/EC), which prescribes that the use of cookies or similar technologies involving the storing of and access to information that is already stored on a user's device (belonging to either a natural or a legal person) is allowed if the users have given their prior informed consent).

In June 2021, the Italian Data Protection Authority adopted new Guidelines on the use of cookies and other tracking tools, which replace the previous guidance provided by it in 2014 and 2015. Most importantly, the new Guidelines confirm that the prior informed consent of the user referred to in article 122 of the Personal Data Protection Code needs to fulfil the validity requirements set forth within articles 4(11) and 7 GDPR (ie, consent must be expressed by means of a clear affirmative action, such as clicking on a button or ticking a box). Therefore, actions such as scrolling or swiping through a webpage, or similar user activity, do not satisfy the requirement of a clear and affirmative action (as indicated by the European Data Protection Board (EDPB) in its Guidelines 05/2020 on consent under Regulation 2016/679).

More specific rules on targeted advertising are currently being discussed at the European level, in the context of the Digital Services Act.

With regard to the targeting of social media users, the EDPB guidelines 08/2020 clarify the roles and responsibilities among the social media provider and the targeters (ie, the natural or legal persons that want to leverage the social media platform to send targeted advertising messages to the users of social media to advance commercial, political or other interests). These guidelines provide many practical examples and aim to identify the potential risks for the rights and freedoms of individuals, the main actors and their roles and describe the application of key data protection requirements (such as lawfulness and transparency, and the necessity to carry out a data protection impact assessment), as well as key elements of arrangements between social media providers and targeters.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Yes. The processing of certain categories of personal data that pertains to intimate aspects (eg, genetic data and data concerning health, or data revealing racial or ethnic origin – 'special categories of personal data') is generally prohibited under article 9(1) of the GDPR. The processing of such data must be grounded on one of the narrow exceptions set forth by article 9(2) GDPR, provided that one of the legal bases set forth by article 6(1) GDPR also applies.

In general, under article 9 GDPR, the general prohibition to process special categories of personal data is lifted where:

- the individual has given explicit consent to the processing of such data for one or more specific purposes;
- the processing of such data is mandated or authorised by the European Union or national law that provides appropriate safeguards for the fundamental rights and the interests of the data subject;
- the processing of such data 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;
- the processing of such data is carried out in the course of 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 the 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 subject;
- the processing of such data relates to personal data that is manifestly made public by the data subject; and
- the processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity.

Similarly, under article 10 GDPR, the processing of personal data relating to criminal convictions and offences should be based on one of the legal bases provided by article 6(1) GDPR and carried out under the control of official authority or when the processing is authorised by the European Union or national law providing for appropriate safeguards for the rights and freedoms of data subjects.

In this respect, article 2-octies of the Personal Data Protection Code specifies and complements article 10 GDPR, providing that where the processing of personal data relating to criminal convictions and offences or related security measures does not take place under the control of official authority, it is permitted only if 'authorized by a law or, in the cases provided for by law, by regulation, which shall provide appropriate guarantees for the rights and freedoms of the data subjects'.

Profiling

44 | Are there any rules regarding individual profiling?

The Italian Data Protection Authority confirmed its consolidated approach that requires, as a rule, the data subjects' consent for profiling purposes. In its Guidelines on promotional activities and the fight against spam, the Authority stated that '[...] As for the purposes for which personal data are processed, it is to be reiterated that a data controller should obtain a specific consent statement for each separate purpose such as marketing, profiling, disclosure of the data to third parties'.

If the data controller leverages profiling to take decisions based solely on automated processing and producing legal effects concerning a natural person, or that similarly significantly affects them, articles 13(2)(f), 14(2)(g), 15(2)(h), 22 and 35 GDPR provide a specific set of rules.

In particular, articles 13(2)(f), 14(2)(g) and 15(2)(h) GDPR provide for specific transparency requirements on the data controller; the latter is required to disclose to the data subject – typically, by means of a privacy notice – the existence of automated decision-making, including profiling, together with 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.

Moreover, pursuant to article 22(1) GDPR, as interpreted by the Article 29 Working Party within the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, such profiling activities are prohibited, except where one of the exceptions set forth under article 22(2) GDPR apply; in other words, where the activity '(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject; or (c) is based on the data subject's explicit consent'.

If the decision is based on the special categories of personal data referred to in article 9(1) GDPR, the activity is lawful only where based on article 9(2) GDPR, letter (a) or (c); in other words, respectively, where the data subjects have provided their explicit consent, or where processing is necessary for reasons of substantial public interest, on the basis of

EU or member state law. In both cases, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must be put in place.

Without prejudice to the above, where the activity is based on letters (a) or (c) of article 22(1) GDPR, the data controller also needs to '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 his or her point of view and to contest the decision'. While the suitable measures are to be assessed and adopted by the data controller on a case-by-case basis, possibly within the context of the data protection impact assessment pursuant to article 35 GDPR, some possible measures are further elaborated within Recital 71 GDPR, thereby including appropriate mathematical or statistical procedures and implementing technical and organisational measures appropriate to ensure, in particular, that factors that result in inaccuracies in personal data are corrected and the risk of errors is minimised, with a view to prevent, inter alia, discriminatory effects.

Furthermore, under article 35(3)(a) GDPR, the use of profiling to take decisions that produce legal effects concerning a natural person or that similarly significantly affect a natural person triggers the obligation for the data controller to perform a data protection impact assessment on the processing operations.

Finally, where profiling is carried out by the data controller through the use of cookies or other tracking technologies, article 122 of the Personal Data Protection Code (transposing the EU e-Privacy Directive 2002/58/EC), prescribes that the use of cookies or similar technologies involving the storing of and access to information that is already stored on a user's device (belonging either to a natural or a legal person), are permitted if the users have given their prior informed consent.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Normal rules set forth by the GDPR and the Personal Data Protection Code apply, as there are no data protection rules specific to cloud computing.

However, rules governing the relationship between data controllers and processors are of particular relevance in this field, considering that the cloud customer typically qualifies as data controller while the cloud provider qualifies as data processor. As a result, pursuant to article 28(1) of the GDPR, the cloud customer must carry out and document the performance of a due diligence on the cloud provider (eg, by submitting and evaluating specific questionnaires), aimed at ascertaining whether the latter can provide a data protection law-compliant solution. In this context, assurances related to the implementation of adequate security measures assume particular importance.

Moreover, the cloud customer and provider must enter into a data processing agreement under article 28(3) of the GDPR.

At the EU level, supervisory authorities adopted Opinion 05/2012 on Cloud Computing, which stresses the cloud client's responsibilities as a controller and recommends that the latter exercises special care and diligence in selecting a provider that guarantees compliance with data protection law, also with regard to the use of sub-providers. The opinion highlights the role that contractual safeguards play in this respect. A specific area of concern in this field is the lawfulness of any cross-border international data transfers outside the European Economic Area, which the cloud customer must map and regulate in accordance with the law.

The Italian Data Protection Authority also issued guidelines in 2012, highlighting the risks involved in implementing cloud solutions (eg, security issues and loss of control over data), and recommending that the cloud client maps the relevant risks before choosing both a suitable cloud solution and which categories of personal data to entrust to the cloud.

Davide Baldini
davide.baldini@ictlc.com

Antonio Landi
antonio.landi@ictlc.com

Paolo Balboni
paolo.balboni@ictlc.com

Luca Bolognini
luca.bolognini@ictlc.com

Floriana Francesconi
floriana.francesconi@ictlc.com

Via Borgonuovo, 12
Milan 20121
Italy
Tel: +39 02 84247194
Fax: +39 02 700512101

Piazza di San Salvatore in Lauro, 13
Rome 00186
Italy
Tel: +39 06 97842491
Fax: +39 06 23328983

Via Ugo Bassi, 3
Bologna 40121
Italy
Tel: +39 051 272036
Fax: +39 051 272036

www.ictlegalconsulting.com

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Italian Data Protection Authority has proven itself to be a rather proactive authority, issuing several significant administrative fines for violations of Regulation (EU) 2016/679 (the EU General Data Protection Regulation) (GDPR), three of which are among the highest monetary penalties issued to date in the European Union. In January 2020, the Italian DPA fined TIM SpA €27.8 million for several instances of unlawful data processing concerning marketing activities that concerned millions of data subjects, including unsolicited marketing calls without having obtained valid consent, contacting data subjects listed in the Public Register of Objections, and for having contacted data subjects who had denied their consent for marketing purposes. On 20 November 2020, the Italian DPA issued another significant fine of €12.25 million to Vodafone Italia SpA, for the unlawful processing of personal data in the context

of direct marketing and telemarketing, with specific regard to the lack of evidence of user consent to the processing, as well as failure on behalf of the company to implement by design appropriate safeguards to prevent such unlawful processing of personal data.

Based on these cases and a more wide-reaching analysis of the fines issued and measures imposed by the Italian Data Protection Authority since the GDPR entered into force, it can be assumed that the Italian Data Protection Authority will continue to closely monitor the adequacy of the selected legal basis for data processing, especially concerning commercial marketing activities, as well as the appropriateness of technical and organisational security measures that are put in place by organisations. It may also be presumed that the Italian Data Protection Authority may be inclined to take a consumer protection perspective in the application of its powers.

Further, the Italian Data Protection Authority recently participated in a joint effort with the antitrust and telecommunication authorities concerning the regulation of big data, publishing a report that provides several recommendations to legislative action in this area. The Italian Data Protection Authority underlined the fact that the technological dimension acquires with big data an impressive ability to explain its effects (not all and not always beneficial) on individuals and society as a whole. Therefore, it is necessary to preserve, (as prescribed in the Italian constitutional system, not unlike that of the European Union), the guarantees acquired over time to protect our fundamental rights as confirmed by the GDPR.

Japan

Akemi Suzuki and Takeshi Hayakawa
Nagashima Ohno & Tsunematsu

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Act on the Protection of Personal Information of 2003, as amended (APPI), sits at the centre of Japan's regime for the protection of PI. Serving as a comprehensive, cross-sectoral framework, the APPI regulates private businesses using PI databases and is generally considered to embody the eight basic principles under the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The APPI is implemented by cross-sectoral administrative guidelines prepared by the Personal Information Protection Commission (the Commission). Concerning certain sectors, such as medical, financial and telecommunications, the Commission and the relevant government ministries have published sector-specific guidance providing for additional requirements given the highly sensitive nature of personal information handled by private business operators in those sectors. Numerous self-regulatory organisations and industry associations have also adopted their own policies or guidelines for the protection of PI.

The APPI has undergone several significant amendments. One of the recent significant amendments was promulgated on 12 June 2020 (the 2020 Amendment) and fully implemented on 1 April 2022. The 2020 Amendment includes, inter alia, a statutory obligation to report certain data breaches to the Commission and notify affected individuals of data breaches that are likely to cause the violation of individual rights and interests.

Another recent amendment was promulgated on 19 May 2021 (the 2021 Amendment) and implemented in part on 1 April 2022 as well and the 2021 Amendment has expanded the scope of the APPI to include rules applicable not only to private sectors but also to governmental sectors.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Personal Information Protection Commission (the Commission) was established on 1 January 2016 as a cross-sectoral, independent government body to oversee the APPI. The Commission has the following powers under the APPI:

- to require reports concerning the handling of PI or anonymised information from private business operators using 'databases, etc' of PI (PI databases), pseudonymised information (pseudonymised information databases), anonymised information (anonymised information databases) or individual-related information (individual-related information databases);
- to conduct an on-site inspection of offices or other premises of private business operators to raise questions and inspect records concerning their handling of PI, pseudonymised information, anonymised information or individual-related information;
- to give 'guidance' or 'advice' necessary for the handling of PI, pseudonymised information, anonymised information or individual-related information to private business operators using PI databases, pseudonymised information databases, anonymised information databases or individual-related information databases;
- upon violation of certain obligations of any private business operator using PI databases, pseudonymised information databases, anonymised information databases or individual-related information databases and to the extent deemed necessary to protect the rights of an affected individual, to 'recommend' cessation or other measures necessary to rectify the violation; and
- if recommended measures are not implemented and the Commission deems an imminent danger to the affected individual's material rights, to order such measures.

The Commission may delegate the power to require reports or conduct an on-site inspection to certain government ministries in cases where the Commission deems it necessary to be able to give guidance or advice effectively. The Commission is also empowered to require reports from, conduct on-site inspections for and order measures against foreign private business operators that are subject to the APPI, signalling the broader extraterritorial application of the APPI.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Under the APPI, in cases where government ministries deem it necessary to ensure the proper handling of personal information, such government ministries may request the Commission to take appropriate measures following the provisions of the APPI.

Also, under the APPI, the Commission may provide foreign authorities enforcing foreign laws and regulations equivalent to the APPI with information that the Commission deems beneficial to the duties of such foreign authorities that are equivalent to the Commission's duties outlined in the APPI. Upon request from the foreign authorities, the Commission may consent that the information provided by it be used for an investigation of a foreign criminal case, subject to certain exceptions.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under the APPI, criminal penalties may be imposed if there has been:

1 failure to comply with any order issued by the Commission (subject to penal servitude of up to one year or a criminal fine of up to ¥1,000,000);
2 failure to submit reports, or submitting of untrue reports, as required by the Commission (subject to a criminal fine of up to ¥500,000);
3 refusal or interruption of an on-site inspection of the offices or other premises by the Commission (subject to a criminal fine of up to ¥500,000); or
4 theft or provision to a third party by any current or former officer, employee or representative of a private business operator of information from a PI database he or she handled in connection with the business of the private business operator for the purpose of seeking unlawful benefits to himself or herself or third parties (subject to penal servitude of up to one year or a criminal fine of up to ¥500,000).

If the foregoing offences are committed by an officer or employee of a subject private business operator that is a judicial entity, then the entity itself may also be held liable for a criminal fine. The amount of the criminal fine for the judicial entity is up to ¥100 million for the offences outlined in (1) and (4) and up to ¥500,000 for the offences outlined in (2) and (3).

Judicial review of data protection authority orders

5 Can PI owners appeal to the courts against orders of the data protection authority?

Administrative law in Japan usually provides for an appeal of a government ministry's decision to a court with proper jurisdiction. Therefore, if the Commission or the relevant government ministry to which powers of the Commission are duly delegated takes administrative actions against a private business operator using PI databases, it will generally be able to challenge the actions judicially.

SCOPE

Exempt sectors and institutions

6 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Act on the Protection of Personal Information of 2003, as amended (APPI) contains notable exemptions for private sectors, as follows:

- In respect of fundamental constitutional rights, media outlets and journalists, religious groups and political parties are exempt from the APPI to the extent of the processing of personal data for purposes of journalism, and religious and political activities, respectively.
- The use of PI for personal purposes is outside the scope of the APPI. The use of PI by not-for-profit organisations or sole proprietorships is within the scope of the APPI.

As for government sectors, there are exemptions to the rights of individuals, such as the right to disclosure, correction and suspension of use of PI concerning criminal cases or the like.

Interception of communications and surveillance laws

7 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Secrecy of communications from the government's intrusion is a constitutional right. Interception of electronic communication by private persons is regulated by the Telecommunications Business Act of 1984 and the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders of 2001. Marketing emails are restricted under the Act on Regulation of Transmission of Specified Electronic Mail of 2002 and the Act on Specified Commercial Transactions of 1976.

Other laws

8 Are there any further laws or regulations that provide specific data protection rules for related areas?

Currently, various local ordinances provide rules for the protection of PI held by local governments; however, from April 2023, these ordinances will also be consolidated into the APPI.

In addition, the Act on Utilisation of Numbers to Identify Specific Individuals in Administrative Process provides rules concerning the use of PI acquired through the use of the individual social security and tax numbering system, My Number.

PI formats

9 What categories and types of PI are covered by the law?

The APPI covers personal information made part of 'databases, etc' of PI (PI databases). 'PI databases' includes electronic databases and manual filing systems that are structured by reference to certain classification criteria so that information on specific individuals is easily searchable.

For purposes of the APPI, 'PI' is defined as information related to a living individual that can identify the specific individual by name, date of birth or other description contained in such information. Information that, by itself, is not personally identifiable but may be easily linked to other information and thereby can be used to identify a specific individual is also regarded as PI. PI also includes signs, code or data that identify physical features of specific individuals, such as fingerprint or face recognition data, or that are assigned to each individual by government or providers of goods or services, such as a driving licence number or passport number. PI comprising a PI database is called personal data.

The APPI provides for three types of data that are distinguished from PI. First, 'anonymised information' means information relating to a particular individual that has been irreversibly processed by applying designated methods for anonymisation such that the individual is no longer identifiable and cannot be reidentified. Anonymised information is not considered personal information, and may be disclosed to third parties without the consent of the relevant individual, provided that the business operator who processes and discloses anonymised information to third parties comply with certain disclosure requirements.

Second, 'pseudonymised information' means information relating to a particular individual that has been processed by erasing or replacing all or part of identifiers in such a manner that the individual is no longer identifiable unless it is collated with other information. In most cases, pseudonymised information is considered personal information. The pseudonymised information may be used for data analysis or other internal use by operators, but it may not be disclosed to third parties except in certain cases.

Third, 'individual-related information' is a concept newly introduced to impose certain additional obligations relating to a transfer of information that is not personally identifiable at the transferor but the transferee can identify the relevant individual by linking such information held by the transferee or otherwise. If a transferor anticipates that the transferee can identify the relevant individual of the data being transferred, the transferor must confirm that the transferee has obtained consent from the relevant individual about the transfer.

Extraterritoriality

10 Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The APPI has an extraterritorial application. Specifically, the APPI applies to foreign private business operators using PI databases, individual-related information databases, pseudonymised information databases or anonymised information databases when they use or process, outside of Japan:

- private business operators handling the PI of individuals residing in Japan in connection with providing goods or services to individuals in Japan; or
- individual-related information to be obtained as such PI, or pseudonymised information or anonymised information produced by such private business operators based on this PI.

Separately, the PI of individuals residing outside of Japan is considered to be protected under the APPI as long as such PI is held by private business operators established or operating in Japan.

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The APPI distinguishes between:

1 obligations imposed on private business operators using PI databases (personal data users); and
2 obligations imposed only on those private business operators using PI databases who control the relevant personal data (PI data owners).

Generally, service providers are subject to the obligations of personal data users but not subject to the obligations of PI data owners.

The obligations of all personal data users mentioned in (1) include:

- to specify the purposes for which the PI is used as explicitly as possible;
- to process the PI only to the extent necessary for achieving such specified purposes unless the relevant individual's prior consent is obtained, subject to limited exceptions;
- to notify the relevant individual of, or publicise, the purposes of use before or at the time of collecting PI unless such purposes were publicised before the collection of the PI;
- not to use PI in a manner that potentially facilitates illegal or unjustifiable conduct;
- not to use deceptive or wrongful means in collecting PI;
- to obtain the consent of the individual before collecting sensitive personal information, which includes race, beliefs, social status, medical history, criminal records and the fact of having been a victim of a crime and disabilities (subject to certain exceptions);
- to endeavour to keep its personal data accurate and up to date to the extent necessary for the purposes of use, and erase, without delay, its personal data that is no longer needed to be used;
- to undertake necessary and appropriate measures to safeguard and protect against unauthorised disclosure of or loss of or damage to the personal data it holds;
- to conduct necessary and appropriate supervision over its employees and its service providers who process its personal data;
- to report to the Personal Information Protection Commission and notify a relevant individual when there is data breach that is likely to harm an individual's rights and interests;
- not to disclose the personal data to any third party without the consent of the individual (subject to certain exemptions);
- to prepare and keep records of third-party transfers of personal data (subject to certain exceptions) (as a result of the 2020 Amendment, including to disclose such records upon the individuals' request, subject to certain exceptions);
- when acquiring personal data from a third party other than data subjects (subject to certain exceptions), to verify the name of the third party and how the third party acquired such personal data; and
- not to conduct cross-border transfers of personal data without the consent of the individual (subject to certain exceptions).

The PI data owners mentioned in (2) have additional and more stringent obligations, which are imposed only in respect to personal data for which a PI data owner has the right to provide a copy of, modify (ie, correct, add or delete), discontinue using, erase and discontinue disclosing to third parties (retained personal data):

- to make accessible to the relevant individual certain information regarding the retained personal data, including:
  - the name and address and, for a corporate body, the name of the representative of the PI data owner;
  - all purposes for which retained personal data held by the PI data owner is generally used;
  - procedures for submitting a request or filing complaints to the PI data owner; and
  - security control measures taken by the PI data owner;
- to provide, without delay, a copy of retained personal data to the relevant individual upon his or her request (subject to certain exceptions);
- to correct, add or delete the retained personal data to the extent necessary for achieving the purposes of use upon the request of the relevant individual (subject to certain exceptions);
- to discontinue the use of or erase such retained personal data upon the request of the relevant individual if such use is or was made, or the retained personal data in question was obtained, in violation of the APPI or if it has become unnecessary to use such retained personal data, a data breach has occurred in connection with such retained personal data, or there is a possibility that handling of such retained personal data would harm the rights or legitimate interests of the relevant individual (subject to certain exceptions); and
- to discontinue disclosure of retained personal data to third parties upon the request of the relevant individual if such disclosure is or was made in violation of the APPI or if it has become unnecessary to use such retained personal data, a data breach has occurred in connection with such retained personal data, or there is a possibility that handling of such retained personal data would harm the rights or legitimate interests of the relevant individual (subject to certain exceptions).

Under the APPI, any personal data where the existence or absence of such personal data would harm the life, body and property of the relevant individual or a third party; encourage or solicit illegal or unjust

acts; jeopardise the safety of Japan and harm the trust or negotiations with other countries or international organisations; or impede criminal investigations or public safety is excluded from the retained personal data and therefore does not trigger the above-mentioned obligations of PI data owners. Under the APPI, any personal data where the existence or absence of such personal data would harm the life, body and property of the relevant individual or a third party; encourage or solicit illegal or unjust acts; jeopardise the safety of Japan and harm the trust or negotiations with other countries or international organisations; or impede criminal investigations or public safety is excluded from the retained personal data and therefore does not trigger the above-mentioned obligations of PI data owners.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Act on the Protection of Personal Information of 2003, as amended (APPI), does not contain specific criteria for legitimate data collection or processing. The APPI does, however, prohibit the collection of PI by deceptive or wrongful means, and requires that the purposes of use must be identified as specifically as possible, and must generally be notified or made available to the relevant individual in advance. In addition, the APPI provides that PI should not be used in a manner that potentially facilitates illegal or unjustifiable conduct. Further, processing of PI beyond the extent necessary for such purposes of use without the relevant individual's prior consent is also prohibited, subject to limited exceptions.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

The APPI imposes stringent rules for sensitive personal information, including race, beliefs, social status, medical history, disabilities, criminal records and the fact of having been a victim of a crime. Collection or disclosure under the 'opt-out' mechanism of sensitive personal information without the consent of the relevant individual is generally prohibited.

Also, the administrative guidelines for the financial sector provide for a similar category of sensitive information. Such information is considered to include trade union membership, domicile of birth and sexual orientation, in addition to sensitive personal information. The collection, processing or transfer of such sensitive information by financial institutions is prohibited, even with the consent of the relevant individual, except under limited circumstances permitted under such administrative guidelines.

Further, in January 2019, upon the decision by the European Commission that Japan ensures an adequate level of protection of personal data under article 45 of the EU's General Data Protection Regulation (GDPR), the supplementary rules regarding the handling of personal data transferred from the European Economic Area based on an adequacy decision by the European Commission (the EEA Data Supplementary Rules) have taken effect. The EEA Data Supplementary Rules impose stringent rules for the personal data transferred from the European Economic Area based on an adequacy decision by the European Commission (EEA data). Upon Brexit, the effect of the adequacy decision by the European Commission has been sustained in the United Kingdom; therefore, EEA data includes the personal data transferred from the United Kingdom and the reference to 'EEA' includes the United Kingdom in this chapter. The Supplementary Rules can be summarised as follows:

1 In cases where EEA data includes data concerning sex life, sexual orientation or trade union membership it is categorised as a special category of personal data under the GDPR, such EEA data is treated as 'sensitive personal information' under the APPI.
2 EEA data is treated as retained personal data under the APPI, regardless of whether or not such EEA data is erased within six months.
3 When a private business operator using PI databases receives EEA data from the European Economic Area, the private business operator is required to confirm and record the purposes of use of such EEA data specified at the time of acquisition from the relevant data subject (original purposes of use).
4 When a private business operator using PI databases receives EEA data from another private business operator who received such EEA data from the European Economic Area, the first private business operator is also required to confirm and record the original purposes of use of such EEA data.
5 In each case of (3) and (4), the private business operator must specify the purposes of use of EEA data within the scope of the original purposes of use of such EEA data, and use such EEA data following such specified purposes of use.
6 When a private business operator using PI databases processes EEA data to create anonymised information under the APPI, the private business operator is required to delete any information that could be used to re-identify the relevant individuals, including any information concerning the method of the process for anonymisation.
7 In cases where a private business operator using PI databases proposes to transfer EEA data it received from the European Economic Area on to a third party transferee located outside of Japan (ie, onward transfer), the private business operator must:
   - provide the data subjects of such EEA data with information concerning the transferee, and obtain prior consent to the proposed cross-border transfer from the data subject; or
   - transfer relying on applicable exemptions of such cross-border transfer.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

There are several notification requirements under the Act on the Protection of Personal Information of 2003, as amended (APPI).

First, the APPI requires all personal data users to notify individuals of, or make available to individuals, the purpose for which their PI is used, promptly after the collection of the PI, unless the purpose was publicised before the collection of the PI. Alternatively, such purpose must be expressly stated in writing if collecting PI provided in writing by the individual directly.

Second, when a private business operator using PI databases is to disclose personal data to third parties without the individual's consent under the 'opt-out' mechanism, one of the requirements that the private business operator must satisfy is that certain information regarding the third-party disclosure is notified, or made easily accessible, to the individual before such disclosure. Such information includes the types of information being disclosed and the manner of disclosure.

Third, when a private business operator using PI databases is to disclose personal data to third parties without the individual's consent

under the 'joint-use' arrangement, the private business operator must notify or make easily accessible, certain information regarding the third-party disclosure before such disclosure. Such information includes items of personal data to be jointly used, the scope of third parties who would jointly use the personal data, the purpose of use by such third parties, and the name and address and, for a corporate body, the name of the representative of a party responsible for the control of the personal data in question.

Fourth, the APPI requires each PI data owner to keep certain information accessible to those individuals whose retained personal data is held. Such information includes:

- the name and address and, for a corporate body, the name of the representative of the PI data owner;
- all purposes for which retained personal data held by the PI data owner is generally used;
- the procedures for submitting a request or filing complaints to the PI data owner; and
- security control measures taken by the PI data owner.

If, based on such information, an individual requests the specific purposes of use of his or her retained personal data, the PI data owner is required to notify, without delay, the individual of such purposes.

Exemptions from transparency obligations

15 | When is notice not required?

There is an exception to the notice requirement imposed on a private business operator using PI databases when collecting PI where among other circumstances:

- such notice would harm the interest of the individual or a third party;
- such notice would harm the legitimate interest of the private business operator; and
- the purposes of use are evident from the context of the collection of the relevant personal data.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

The APPI requires all private business operators using PI databases to endeavour to:

- keep the personal data they hold accurate and up to date to the extent necessary for the purposes for which the personal data is to be used; and
- erase, without delay, such personal data that is no longer needed.

As a result of the 2020 Amendment, PI data owners must, upon the relevant individual's request, discontinue the use of or erase retained personal data that is no longer needed.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The APPI does not restrict the types or volume of PI that may be collected, other than restricting the collection of sensitive personal information without obtaining the consent of the relevant individual. Sensitive personal information includes information on race, beliefs, social status, medical history, disabilities, criminal record and the fact of having been a victim of a crime.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

No. Personal data may be held as long as is necessary for the purposes for which it was collected. Under the APPI, private business operators using PI databases must endeavour to erase, without delay, such personal data that no longer needs to be used.

In addition, as a result of the 2020 Amendment, such private business operators must, upon the relevant individual's request, discontinue the use of or erase retained personal data that is no longer needed.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI can generally be used only to the extent necessary to achieve such specified purposes as notified or made available to the relevant individual. Use beyond such extent or for any other purpose must, in principle, be legitimised by the consent of the relevant individual.

Exemptions from the purposes for use requirement apply to, for instance, the use of PI pursuant to laws, and where use beyond specified purposes is needed to protect life, body and property of a person and it is difficult to obtain the consent of the affected individual.

In addition, under the APPI, the purpose for use may be amended, without the consent of the relevant individual, to the limited extent that would be reasonably deemed to be related to the previous purposes.

PI may be used for such amended purposes, provided that the amended purposes be notified or made available to the affected individuals.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The APPI does not restrict the use of PI for automated decision-making, and PI can generally be used to the extent necessary to achieve such specified purposes as notified or made available to the relevant individual.

However, the APPI requires that the purpose of use should be specified as explicitly as possible. In this regard, the Personal Information Protection Commission explains in one of its cross-sectoral administrative guidelines for the APPI that when analysing information, such as behaviours and interests related to an individual from the information obtained from the individual, private business operators using PI databases must specify the purpose of the use to the extent that such individual can predict and assume what kind of processing will be performed.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Act on the Protection of Personal Information of 2003, as amended (APPI) provides that all personal data users must have in place 'necessary and appropriate' measures to safeguard and protect against unauthorised disclosure of or loss of or damage to the personal data they hold or process; and conduct necessary and appropriate supervision over their employees and service providers who process such personal data. What

constitutes 'necessary and appropriate' security measures is elaborated on in the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines). The Commission Guidelines set forth a long list of four types of mandatory or recommended security measures – organisational, personnel, physical and technical – as well as the requirement to adopt internal security rules or policies. The Commission Guidelines also require that, when private business operators using PI databases handle personal data in a foreign country, they must take necessary and appropriate measures for the security control of personal data after understanding the personal information protection regime of such foreign country.

In addition, some of the sector-specific guidelines, such as the administrative guidelines for the financial sector, provide for more stringent requirements on security measures.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Under the APPI, private business operators are required to report to the Commission and notify affected individuals of a data breach that is highly likely to harm the rights and interests of affected individuals. A leakage, loss or damage of personal data constitutes such a data breach.

The enforcement rules provide that such reporting obligation will be triggered if:

- a data breach of sensitive personal information has occurred or is likely to have occurred;
- a data breach that may cause financial damage due to unauthorised use has occurred, or is likely to have occurred;
- a data breach that may have been committed with a wrongful purpose has occurred or is likely to have occurred; and
- a data breach where more than 1,000 data subjects have been or are likely to be affected.

As for reporting to the Commission, a business operator will be required to make both 'prompt reporting' and 'confirmatory reporting.' When becoming aware of a data breach of any of the categories mentioned above, a business operator must 'promptly' report to the Commission based on its knowledge of the data incident at that time. The 'promptly' is construed to approximately be three to five days. Subsequently, the business operator must make confirmatory reporting within 30 days (or 60 days if the data breach may have been committed for a wrongful purpose).

As for notification to affected data subjects, the enforcement rules require that the business operator notify them 'promptly in light of the relevant circumstances'. Unlike the obligation to report to the Commission, the business operator may be exempted from so notifying if it is difficult to notify them and sufficient alternative measures are taken to protect their rights and interests.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Under the Act on the Protection of Personal Information of 2003, as amended (APPI), private business operators using PI databases (regardless of whether they are owners or processors of PI) are obliged to take necessary and appropriate measures for the security control of personal data. According to the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines), such necessary and appropriate measures include the following:

- to establish basic policies that declare the stance of the private business operator towards taking necessary and appropriate measures for the control of personal data;
- to establish internal rules with respect to the handling of personal data;
- to implement organisational, personal, physical and technical control measures; and
- to take necessary and appropriate measures for the control of personal data after understanding the personal information protection regime of a foreign country, when handling personal data in such a foreign country.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There is no statutory requirement to appoint a data protection officer. However, the appointment of a 'chief privacy officer' is generally recommended under the Commission Guidelines. The Commission Guidelines do not provide for the qualifications, roles or responsibilities of a chief privacy officer.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Under the APPI, private business operators using PI databases that have disclosed personal data to third parties must generally keep records of such disclosure. Also, private business operators receiving personal data from third parties rather than the relevant individuals must generally verify how the personal data was acquired by such third parties and keep records of such verification.

The foregoing obligation does not apply to the disclosure of personal data to outsourced processing service providers, as part of mergers and acquisitions transactions or for joint use, as long as the disclosure is not based on consent regarding the cross-border transfer restrictions.

Risk assessment

26 Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The APPI does not oblige private business operators using PI databases (regardless of whether they are owners or processors of PI) to carry out risk assessments in relation to the use of PI.

However, the APPI requires private business operators to take necessary and appropriate measures for the security control of personal data as well as supervise their employees and outsourced service providers. In this regard, it is recommended under the Commission Guidelines that such appropriate measures and supervision be conducted in accordance with the risks arising from the nature and size of the business, status of use of the PI (including the nature and quantity of PI) and the media on which PI is recorded. Therefore, to implement the appropriate measures for security control, it is expected under the APPI that private business operators will implement risk assessments in connection with such aspects.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

No. However, the Commission Guidelines generally require that, when implementing security measures to safeguard the personal data it holds or processes, each private business operator using PI databases should consider the degree of the impact of any unauthorised disclosure or another incident on the right or interest of one or more data subjects affected by such an incident.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Under the Act on the Protection of Personal Information of 2003, as amended (APPI), personal data users who disclose personal data (other than certain personal data such as sensitive personal information) under the 'opt-out' mechanism are required to submit a notification to the Personal Information Protection Commission (the Commission) before such disclosure. According to the Commission, the primary target of this requirement is mailing list brokers.

Notification to the Commission regarding the opt-out mechanism should include certain matters, such as the categories of personal data to be disclosed, the method of disclosure, how the relevant individual may request to cancel such opt-out disclosure to the private business operators and other designated matters. No penalties are statutorily provided for the failure to submit notification of such opt-out disclosure.

Other transparency duties

29 | Are there any other public transparency duties?

Apart from the matters required under the APPI to notify individuals as separately mentioned in this chapter, the Commission Guidelines recommend that private business operators using PI databases make public an outline of the processing of personal data such as whether the private business operators outsource the processing of personal data and the contents of the processing to be outsourced.

Also, the administrative guidelines for the financial sector recommend that private business operators using PI databases make public:

- the purpose of the use of personal information specified according to the types of customers;
- whether the private business operators outsource the processing of personal data;
- the contents of the processing to be outsourced;
- the sources and methods of obtaining personal information; and
- a statement to the effect that upon the request of individuals, the use of retained personal data will be discontinued.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Act on the Protection of Personal Information of 2003, as amended (APPI) generally prohibits disclosure of personal data to third parties without the relevant individual's consent. As an exception to such prohibition, the transfer of all or part of personal data to persons that provide outsourced processing services is permitted to the extent such services are necessary for achieving the permitted purposes of use. Private business operators using PI databases are required to engage in 'necessary and appropriate' supervision over such service providers to safeguard the transferred personal data. Necessary and appropriate supervision by private business operators is generally considered to include:

- proper selection of service providers;
- entering into a written contract setting forth necessary and appropriate security measures; and
- collecting necessary reports and information from the service providers.

The APPI does not set forth specific contractual obligations that must be included in the above contract. However, in practice, it is desirable for certain matters to be included in the contract, such as matters for the control of personal data, sub-processing, reports from the service providers, confirmation of the compliance of the contract (such as information security auditing), measures in the case of non-compliance with the contract and communications in the case of a data breach.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

In principle, the APPI prohibits sharing of PI to a third party without the individual's consent. Important exceptions to the general prohibition include the following, in addition to sharing for outsourced processing services, the following restrictions apply.

Disclosure under the 'opt-out' mechanism

A private business operator using PI databases may share personal data with third parties without the individual's consent, provided that:

- it is prepared to cease such sharing upon request from the individual;
- certain information regarding such sharing is notified, or made easily accessible, to the individual before such disclosure; and
- such information is notified to the Personal Information Protection Commission (the Commission) in advance.

Transfer in mergers and acquisitions transactions

Personal data may be transferred without the consent of the individual in connection with the transfer of a business as a result of a merger or other transactions.

Sharing for joint use

A private business operator using PI databases user may disclose personal data it holds to a third party for joint use, provided that certain information regarding such joint use is notified, or made easily accessible, to the individual before such disclosure. Such disclosure is most typically made when sharing customer information among group companies to provide seamless services within the permitted purposes of use. Information required to be notified or made available includes items of personal data to be jointly used, the scope of third parties who would jointly use the personal data, the purpose of use by such third parties, and the name and address and, for a corporate body, the name of the representative of a party responsible for the control of the personal data in question.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The APPI does not stipulate any supervisory authority notification requirements nor authorisation requirements. Under the APPI, the

transfer of personal data to a third party located outside Japan is generally subject to the prior consent of the relevant individual, subject to the important exceptions mentioned below.

First, no prior consent of the relevant individual is required if the third party is located in a foreign country that the Commission considers has the same level of protection of personal information as Japan. On 23 January 2019, countries in the European Economic Area were designated as such by the Personal Information Protection Commission in exchange for the parallel decision by the European Commission that Japan ensures an adequate level of protection of personal data under article 45 of the General Data Protection Regulation. Such designation by the Commission covers the United Kingdom after Brexit.

The second exception is applicable where the relevant third-party transferee has established a system to continuously ensure its undertaking of the same level of protective measures as private business operators using PI databases would be required under the APPI. According to the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines), for this exception to apply, the private business operator and the foreign third party may ensure in a contract that:

- the third party undertakes such protective measures; and
- if the third party is an intra-group affiliate, the data user and the foreign third party may rely on a privacy statement or internal policies applicable to the group that are appropriately drafted and enforced.

Also, this exception is generally applicable if the foreign third party has certification from an internationally recognised framework of protection of personal data; specifically, certification under the Asia-Pacific Economic Cooperation's Cross Border Privacy Rules system.

In addition, the 2020 Amendment, which fully took effect on 1 April 2022, has imposed enhanced obligations on cross-border transfer. First, when obtaining prior consent to the cross-border transfer from data subjects whose data is to be transferred overseas, the private business operator must provide them with the name of the foreign country where the relevant PI is transferred to, the personal information protection system of the foreign country and actions to be undertaken by the relevant third-party transferees for the protection of personal information.

Also, regarding the above second exception, the 2020 Amendment has introduced that the transferor shall periodically monitor the status of implementation by the foreign third-party transferee of protective measures and any system of the foreign country that may affect the implementation measures, and take necessary and appropriate measures if the implementation of such protective measures is hindered. Upon request of affected data subjects, the transferor will also be required to provide them with information useful to the data subjects.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions on the cross-border transfers of PI under the APPI are equally applicable to transfers to service providers. They may also apply to onward transfers in the sense that the initial private business operators must ensure that not only the transferors of such onward transfers but also their transferees adhere to the cross-border restrictions of the APPI.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no statutory requirement under the APPI that data should be stored in Japan. This requirement, however, exists in certain limited industries. For instance, under the Security Guidelines for Providers of Information Systems and Services involving Medical Information, information system and service providers that process medical information are required to have these systems and services and the relevant medical information 'within the territorial jurisdiction of Japanese law'.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Act on the Protection of Personal Information of 2003, as amended (APPI), individuals have the right to require disclosure of their PI held by PI data owners. Specifically, upon request from individuals, PI data owners are obligated to disclose, without delay, retained personal data of the requesting individuals (the obligation of disclosure). Such disclosure, however, is exempted as a whole or in part if such disclosure would:

- prejudice the life, body, property or other interest of the individual or any third party;
- cause material impediment to the proper conduct of the business of the PI owners; or
- result in a violation of other laws.

Other rights

36 | Do individuals have other substantive rights?

Under the APPI, individuals have the right to require, and PI data owners are obliged to:

- correct, add or delete the retained personal data to the extent necessary for achieving the purposes of use – the obligations of correction etc;
- discontinue the use of or erase the retained personal data if such use is or was made, or the retained personal data in question was obtained, in violation of the APPI (subject to certain exceptions) – the obligation of cessation of use, etc); and
- discontinue disclosure to third parties of retained personal data if such disclosure is or was made in violation of the APPI (subject to certain exceptions) – the obligation of cessation of third-party disclosure.

Also, PI data owners are subject to an obligation to cease disclosure of personal data to third parties if the relevant individual 'opts out' of the third-party disclosure.

In addition, as a result of the 2020 Amendment, individuals also have the right to require PI data owners to discontinue the use of or erase, or discontinue disclosure to third parties, of retained data, if the data is no longer needed, the data was divulged in a data incident or the processing of the data may result in violation of the individual's rights and interests.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The APPI does not provide for individuals' statutory right to receive compensation or the private business operators' obligation to compensate individuals upon a breach of the APPI. However, under the civil code of Japan, an individual may bring a tort claim based on the violation of his or her privacy right. Breaches of the APPI by a PI data owner will be a factor as to whether or not a tortious act existed. If a tort claim is granted, not only actual damages but also emotional distress may be compensated to the extent reasonable.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals' right to monetary compensation is enforced through the judicial system. Concerning violations by PI data owners of the obligations to respond to individuals' requests as separately mentioned in this chapter (ie, obligations of disclosure, correction, etc, cessation of use, etc, and cessation of third-party disclosure), individuals may exercise their rights to require PI data owners to respond to such requests through the judicial system, provided that they first request the relevant PI data owners to comply with such obligations and two weeks have passed after such request was made. Separately, the Personal Information Protection Commission may recommend PI data owners to undertake measures necessary to remedy such violations if it deems it necessary to do so for the protection of individuals' rights.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

No.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

There are no binding rules applicable to the use of 'cookies' or equivalent technology. Any data collected through the use of cookies is generally considered not to be personally identifiable by itself. If, however, such data can be easily linked to other information and thereby can identify a specific individual, then the data will constitute personal data subject to the Act on the Protection of Personal Information of 2003 (APPI), as amended.

Also, the 2020 Amendment, which fully took effect on 1 April 2022, has introduced the concept of 'individual-related information'. Individual-related information means information concerning an individual that is not personal information, pseudonymised information, or anonymised information for a transferor but a transferee can identify the relevant individual by linking such transferred information with the PI held by the transferee. In the context of cookies sync, when if they are not personally identifiable for a transferor but are expected to be synched and used by a transferee as personal data, these cookies would constitute 'individual-related information', and the transferor must confirm that the transferee has obtained consent from the relevant individual to the collection of such data as personal data.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Unsolicited marketing by email is regulated principally by the Act on Regulation of Transmission of Specified Electronic Mail. Under the Act, marketing emails can be sent only to a recipient who:

- has 'opted in' to receive them;
- has provided the sender with his or her email address in writing (eg, by providing a business card);
- has a business relationship with the sender; or
- makes his or her email address available on the internet for business purposes.

Also, the Act requires the senders to allow the recipients to 'opt out'. Marketing emails sent from overseas will be subject to this Act as long as they are received in Japan.

Unsolicited telephone marketing is also regulated by different statutes. It is generally prohibited to make marketing calls to a recipient who has previously notified the caller that he or she does not wish to receive such calls.

Targeted advertising

42 | Are there any rules on targeted online advertising?

The APPI does not have specific rules on targeted online advertising. In addition, any data collected through the use of cookies or equivalent technology for the purpose of targeted online advertising is generally considered not to be personally identifiable by itself. If, however, such data can be easily linked to other information and can thereby identify a specific individual, the data will constitute personal data subject to the APPI, as amended.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The APPI imposes stringent rules for sensitive personal information, including race, beliefs, social status, medical history, disabilities, criminal records and the fact of having been a victim of a crime. Collection or disclosure under the opt-out mechanism of sensitive personal information without the consent of the relevant individual is generally prohibited.

Also, the administrative guidelines for the financial sector provide for a similar category of sensitive information. This information is considered to include trade union membership, domicile of birth and sexual orientation, in addition to sensitive personal information. The collection, processing or transfer of such sensitive information by financial institutions is prohibited, even with the consent of the relevant individual, except under limited circumstances permitted under such administrative guidelines.

Profiling

44 | Are there any rules regarding individual profiling?

The APPI does not have specific rules on individual profiling. However, private business operators are required to specify the purposes for which the PI is used as explicitly as possible under the APPI. In this regard, the Personal Information Protection Commission explains in the cross-sectoral administrative guidelines for the APPI, which were amended on 1 April 2022, that when analysing information, such as behaviours and

interests related to an individual from the information obtained from the individual, private business operators using PI databases must specify the purpose of the use to the extent that such individual can predict and assume what kind of processing will be performed.

Also, the administrative guidelines for the telecommunication sector further provide that when information equivalent to sensitive personal information is generated as a result of profiling, it is recommended for private business operators in the telecommunication sector to obtain the consent of the relevant individuals in advance, and it is also recommended for such private business operators not to use such information unnecessarily for advertisement distribution without obtaining the consent of the relevant individuals.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The Personal Information Protection Commission (the Commission) has published its stance that the use of cloud server services to store personal data does not constitute disclosure to outsourced processing service providers as long as it is ensured by contract or otherwise that the service providers are properly restricted from accessing personal data stored on their servers. If the use of a particular cloud computing service is considered to constitute disclosure to outsourced processing service providers, private business operators using PI databases are required to engage in 'necessary and appropriate' supervision over the cloud service providers to safeguard the transferred personal data. Additionally, private business operators need to confirm that the service providers, if the servers are located outside of Japan, meet the equivalency test so as not to trigger the requirement to obtain prior consent from the individuals to the cross-border transfer of data.

Also, the cross-sectoral administrative guidelines for the APPI published by the Commission, which were amended on 1 April 2022, newly elaborate that when private business operators using PI databases handle personal data in a foreign country (including storing personal data in the servers located outside of Japan), they must take necessary and appropriate measures for the security control of personal data after understanding the personal information protection regime of such foreign country.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Act on the Protection of Personal Information of 2003 (APPI) has recently undergone several significant amendments. One of the recent significant amendments was promulgated on 12 June 2020 (the 2020 Amendment) and fully implemented on 1 April 2022. The 2020 Amendment includes, inter alia, a statutory obligation to report certain data breaches to the Personal Information Protection Commission and notify affected individuals of data breaches that are likely to cause the violation of individual rights and interests.

Another recent amendment was promulgated on 19 May 2021 (the 2021 Amendment) and implemented in part on 1 April 2022. The 2021 Amendment expanded the scope of the APPI to include rules applicable not only to private sectors but also to government sectors.

NAGASHIMA OHNO & TSUNEMATSU

Akemi Suzuki
akemi_suzuki@noandt.com

Takeshi Hayakawa
takeshi_hayakawa@noandt.com

JP Tower
2-7-2 Marunouchi
Chiyoda-ku
Tokyo 100-7036
Japan
Tel +81 3 6889 7000
www.noandt.com

Jordan

Ma'in Nsair, Haya Al-Erqsousi, Mariana Abu-Dayah and Odai Oqlat

Nsair & Partners - Lawyers

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The protection of PI requires a response to rapid technological developments relating to the use of digital devices, computers and anything connected to the internet. The PI of individuals is no longer limited to name, photo and phone number, but has expanded to include other vital data, including fingerprints, health data and geographic location. The system of legislation and laws in this area seeks to protect the PI of individuals in the banking, the telecommunications and many other sectors.

Currently, no enforceable law exists in Jordan for the protection PI. However, a bill (the Bill) has been presented to Parliament that addresses many of the principles and rules stipulated in the Organization for Economic Co-operation and Development guidelines, Convention 108, EU Directive 95/46/EC and the European Convention on Human Rights, as well as fundamental freedoms such as those pertaining to notice, purpose, agreement, safety and disclosure. It also deals with the rules imposed in the EU General Data Protection Regulation, such as the right to be forgotten and the right of consent.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

According to article 2 of the Bill, the provisions will establish a council for the protection of PI, which in turn will establish a PI unit in the Ministry of Digital Economy and Entrepreneurship. This organisational unit is competent to protect PI in the Ministry of Economy and Entrepreneurship, utilising the powers specified under article 18 of the Bill, including:

- preparing draft legislation and instructions related to the protection of PI;
- receiving reports and complaints related to violations;
- investigating the perpetrators of violations and making appropriate decisions on these matters;
- monitoring the commitment of any person responsible for data processing, and the extent of their commitment to specific technical and administrative procedures;
- monitoring compliance with the provisions of the law, regulations and instructions; and
- opening, supervising and organising an official registry of PI officials, processors and controllers.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Article 15 of the Bill stipulates the regional or international judicial cooperation under international agreements or treaties in force in Jordan, in addition to international or regional cooperation between Jordan and international or regional bodies, organisations or agencies working in the field of combating crime of all kinds, including the prosecution of perpetrators.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

According to articles 20 and 21 of the Bill, specific penalties are available to the PI protection unit in response to any violation of the Bill and the regulations and instructions issued according to it, and in proportion to the degree of the violation. Initially, the unit will have the authority to issue a warning that the violation must be stopped within a certain period. If the period lapses without due compliance with the warning, the council for the protection of PI, based on the PI unit's recommendation, has the authority to suspend, stop or withdraw the licence, as well as the power to impose daily fines not exceeding 500 Jordanian dinars per day. In addition, financial penalties of not less than 1,000 Jordanian dinars, and not more than 10,000 Jordanian dinars, may be imposed on those who violate the provisions of the law. The court may also rule to destroy the PI or cancel the PI subject of any case in which a conviction decision was issued.

Judicial review of data protection authority orders

5 Can PI owners appeal to the courts against orders of the data protection authority?

PI owners can appeal all administrative decisions made by the supervisory authority before the administrative court. Any decision of the administrative court is subject to subsequent appeal before the Jordanian High Administrative Court.

SCOPE

Exempt sectors and institutions

6 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The proposed bill to protect PI (the Bill) deals only with information relating to natural persons. It also addresses the sensitive PI pertaining

to the protection of a person's life. However, certain areas of activity (such as national security) are outside the scope of this legislation.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Bill covers the protection of geolocation data. The rules for intercepting communications fall under the remit of the Jordanian Telecommunications Law, which aims to cover and protect the field of communications in all forms.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Specific provisions for the protection of data can also be found in the Communications Law, the Banking Secrecy Law, the Penal Law and the Public Health Law.

PI formats

9 | What categories and types of PI are covered by the law?

The Bill seeks to ensure the protection of any PI, regardless of its source or form, that would identify a natural person directly or indirectly, including data related to personal status, family status or geolocation data. The Bill also includes the provisions on the protection of sensitive PI for natural persons, which is defined as data that directly or indirectly indicates:

- ethnic origin;
- race;
- opinions;
- basic affiliations;
- religious beliefs;
- financial status;
- health (physical or mental condition);
- the presence of a criminal record; or
- any other information that the Personal Data Protection Board deems sensitive.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

No, the provisions of the Bill are applicable to any PI processing of natural persons inside Jordan, even if the owner is located outside Jordan, including the transfer and exchange of PI inside and outside Jordan.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Yes, the processing of PI is conducted in any form and for the purpose of collecting, accessing, recording, copying, saving, storing, organising, revising, exploiting, using, sending, distributing, publishing, transmitting, displaying, anonymising, encoding, or destroying it, or linking to other data or making it available. The owner is the natural or legal entity, whether inside or outside Jordan, who has the PI in his or her custody.

The processor is the natural or legal entity who oversees PI processing.

Finally, the controller is any natural or legal entity, whether inside or outside Jordan, to whom the owner transfers or with whom the owner exchanges PI.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes, the processing of PI is conducted in any form or for the purpose of collecting, accessing, recording, copying, saving, storing, organising, revising, exploiting, using, sending, distributing, publishing, transmitting, displaying, anonymising, encoding or destroying it, or linking it to other data or making it available. The owner is the natural or legal entity, whether inside or outside Jordan, who has the PI in his or her custody.

The processor is the natural or legal entity who oversees PI processing.

Finally, the controller is any natural or legal entity, whether inside or outside Jordan, to whom the owner transfers or with whom the owner exchanges PI.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

According to article 4 of the proposed bill to protect PI (the Bill), PI may not be processed except after obtaining the prior consent of the individual whose PI is being processed or in cases authorised by law. Unless the processing is legal and legitimate, it may not be carried out without obtaining the consent of the individual concerned and must be in accordance with the provisions specified in article 6 of the Bill.

Additionally, article 5 of the Bill imposes the conditions of prior approval, namely:

- that prior approval must be explicit and documented in writing or electronically;
- that it be specific in terms of duration and purpose;
- that the request be in clear, simple, non-misleading and easily accessible language; and
- that there is approval of one of the parents or guardians of an individual who does not have legal capacity or the approval of the judge at the request of the PI unit at the Ministry of Digital Economy and Entrepreneurship if it is in the best interest of those who do not have the legal capacity.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

According to article 9 of the proposed bill to protect PI (the Bill), the owner must, before starting processing, inform the individual concerned in writing or electronically of the following:

- the PI that will be processed;
- the date that processing will commence;
- the purpose for which the PI is being processed; and
- the time period during which the PI will be processed, provided that the PI is not extended.

The time period is provided only with the consent of the individual concerned and the processor, who will include the owner in the execution of the processing, and when permitted by the security and safety controls for PI protection and information on the identification.

Exemptions from transparency obligations

15 | When is notice not required?

According to article 6 of the Bill, the processing of PI may be carried out without having obtained the consent of the individual concerned if the processing is conducted directly by a competent public authority in the fulfilment of tasks entrusted to it by law or through other parties to which it is contracted, provided that the contract includes observance of the obligations stipulated in the law and if they meet one or more of the following conditions:

- if carried out for preventive medical purposes, for medical diagnosis or for providing care by the licensee;
- if it would enable the protection of the life of the individual concerned or protect his or her vital interests;
- if deemed necessary by a competent authority for the detection or prevention of a crime or to prosecute crimes committed contrary to the provisions of the law;
- if required or authorised by any legislation or by a decision of the court;
- if necessary for the purposes of scientific or historical research, provided that its purpose is not to make a decision or take an action regarding a specific person;
- if necessary for statistical purposes, for national security requirements or for the public interest; or
- if the processing of PI is publicly available from the individual concerned.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

According to article 7 of the Bill, PI should be accurate and subject to periodic updating to ensure that it is the same upon each use, as well as to verify that the purpose of the processing is legitimate, specific and clear, and that any subsequent procedure is conducted in a manner that is consistent with the purpose for which it was collected, through legitimate means. The processing should be carried out in a way that does not determine the individual and does not lead to the harm of individuals from whom the data was collected or undermine their rights or freedoms, in accordance with the law and in a way that ensures the confidentiality of PI and the avoidance of any amendments being made to such PI.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The Bill does not explicitly restrict the types or volume of PI that may be collected. However, it is implicitly understood that collected PI must be used solely for the purpose of data processing and any data that is not related to this purpose shall be exempted and not be collected.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The Bill restricts the amount of PI that may be held and the duration for which it may be retained for the purpose of data processing. Held PI may not exceed the required amount for the purpose of fulfilling data processing and must not be held for any period exceeding the time frame defined for data processing or until it has been delivered to the person in whose custody the data belongs, unless the time frame is extended upon the approval of the concerned individual.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Data processors must use the collected PI only for the purposes for which the PI has been collected, as the Bill has adopted the finality principle. Therefore, PI must not be processed for purposes other than those for which it was collected, unless the consent of the individual has been obtained, or as explicitly permitted or required by law.

The Bill stipulates that when a data processor wishes to use the held PI for a new purpose, prior consent must be obtained from the concerned individuals for their PI to be used for the newly identified purpose. Moreover, the exceptions from the finality principle limit usage to only that which is required or permitted by law.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The Bill does not refer to automated decision-making; however, the Bill has provided concerned individuals the right to object to the data processing and its outcome. In addition, according to article 19 of the Credit Information Act, the concerned individual has the right to object regarding any credit information contained in their credit report.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The proposed bill to protect PI (the Bill) stipulates that data and the subject matter of data processing are confidential. Therefore, the legislation imposes general obligations on data controllers and processors to protect PIs from any disclosures or misuse, including – without limitation – ensuring the safety and security of PI from any breach or disclosure, and the development of appropriate means to detect and trace attacks and threats on PI security.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

According to article 2 of the Bill, a data breach denotes any unauthorised access or operation, transfer or action on the data. The Bill requires data processors to notify the supervisory authority and concerned individuals of their data breach only if the consequences would cause great damage to the PI of concerned individuals. This notification and its time frame are largely dependent on the recipients, as the data processors must notify concerned individuals within 24 hours of the breach or disclosure discovery, informing them of the discovery of the breach and providing any advice to be taken to avoid any consequences.

Furthermore, the data processor must notify the supervisory authority within 72 hours of the breach or disclosure discovery. This notification must include the source of breach, its mechanism and the names of the concerned individuals whose data may have been breached or disclosed. If any of that information is unavailable within the period in question, then the data processor must inform the supervisory authority and update them when the information becomes available.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The proposed bill to protect PI (the Bill) stipulates the minimum requirements and rules with which each owner or processor of PI must comply, as well as the requests from such entities regarding the techniques and procedures to be used in PI processing. Even if the owners or processors have not set those internal controls or techniques, they must comply with the Bill, otherwise the breaching party shall be subject to sanctions.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

In general, according to the Bill, data processors are obliged to appoint a data protection officer who has the capability to abide by their legal responsibilities, especially in the following circumstances:

- if the main activity of the data processor is data processing;
- when processing sensitive PI;
- when processing an incompetent person's PI;
- when processing PI related to credit information;
- when transferring PI outside Jordan; or
- in other circumstances defined by the council for the protection of PI.

With regard to the legal responsibilities of the data protection officer, these include – without limitation – the following:

- monitoring all procedures taken by the data processor regarding PI protection and authenticating compliance with the Bill and any related laws;
- supervising the periodic evaluation and examination of personal data base systems, personal data processing systems, and systems for maintaining the security and protection of personal data, provided that the data protection officer documents the results of the evaluation, issues the necessary recommendations for the protection of PI and follows up on the implementation of these recommendations;
- working as a direct liaison officer with the supervisory authority and the security and judicial authorities regarding compliance with the provisions of the Bill;
- developing internal instructions and policies for receiving and examining complaints, requests for data access, and requests for the correction or deletion of data;
- monitoring the adequacy of the technological means used to enable the concerned individuals to exercise their rights; and
- organising training programmes for PI processing for data processors' employees to qualify them to deal with PI in full compliance with the requirements of the Bill.

According to the Bill, a data protection officer must be a natural person and capable of complying with the legal responsibilities as outlined above.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Data processors are obliged by the Bill to set and establish manuals and guidelines that stipulate all followed procedures and policies for data processing and how complaints are being monitored by the data controllers and processors. Data processors must also keep complete records of the data transferred to any entity, the purpose of the transfer, and the approval of concerned individuals.

Risk assessment

26 Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

According to the Bill, data processors through data protection officers, must supervise the periodic evaluation and examination of personal database systems, personal data processing systems and systems for maintaining the security and protection of personal data, provided that the data protection officer documents the results of the evaluation, issues the necessary recommendations for the protection of PI and follows up on the implementation of these recommendations.

Design of PI processing systems

27 Are there any obligations in relation to how PI processing systems must be designed?

Separate articles of the Bill stipulate certain obligations regarding privacy by design, as the Bill obliges data processors to ensure the security and privacy of PI. However, data processors are not obliged to comply with formal protocols regarding data encryption. Data processors must always operate on a legal basis, must delete data that are no longer in use, and are restricted from sharing, transferring or using personal data, except for the purposes of data processing and with the consent of concerned individuals.

While it is not explicitly stated that a privacy impact assessment must be carried out before data processing, data processing must not cause damage to individuals from whom data has been collected, or infringe their rights or freedoms according to the guidelines stipulated in the regulation, which must be issued and published according to the Bill.

REGISTRATION AND NOTIFICATION

Registration

28 Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

The proposed bill to protect PI (the Bill) refers to systems and regulations that shall be issued to define types of permits and approvals, procedures for suspension or revocation, entities exempted from obtaining such permits and approvals, and the fees for its issuance and renewal. Those systems and regulations have not been published yet, meaning registration formalities have not been set at this stage.

Other transparency duties

29 | Are there any other public transparency duties?

According to the Bill, all policies and guidelines that are set by data processors when processing and collecting data must be published to the public through the data controllers and processors' websites.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

According to the proposed bill to protect PI (the Bill), all data controllers and data processors, as well as any third parties who provide processing services, are subject to the same duties and legal responsibilities as further detailed. According to the Bill, data processor or owners, prior to transferring data, must be assured of the security and measures to be taken by the outsourced processor.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Disclosure of any PI between the data processor and any third parties is restricted without the prior consent of the data subject. Additionally, the prior consent of the data subject does not allow personal information to be sold or shared for online targeted advertising purposes, except with the explicit agreement of the data subject.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

According to the Bill, any cross-border transaction of PI must be transferred to a party that has a sufficient level of data protection. The level of protection afforded to a data recipient is equivalent to that imposed by Jordanian laws and regulations, except in the following cases:

- judicial cooperation is established under international conventions and treaties;
- international cooperation in the field of combating crimes;
- data exchange is essential for patient treatment;
- data exchange is related to epidemiological and health disasters;
- the data subject has approved the transfer of data after being made aware that the level of protection outside the jurisdiction is not equivalent to the level imposed by Jordanian laws and regulations; and
- transfer of funds abroad.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Authorisation is not required for transfers to service providers or onwards transfers.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

Retaining PI or a copy of PI is prohibited by the Bill. Data must be deleted as soon as related processing is completed.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals (data subjects) have the right to access and update their personal information from time to time and as appropriate. However, individuals do not have a right to access and update this information if it is only stored for security reasons and if it is not available to the public.

Other rights

36 | Do individuals have other substantive rights?

The proposed bill to protect PI (the Bill) gives individuals many rights, such as the right:

- to access;
- to object and withdraw the acceptance of processing;
- to be informed;
- to receive rectification and restriction of processing;
- to data portability;
- to be forgotten; and
- to ensure data erasure.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

According to the Bill and tort and civil law, individuals are entitled to monetary damages for harm and damage caused by data processors and data controllers. The civil law and tort provisions cover the actual damage, as well as damage for emotional distress.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Both the supervisory authority and the judicial system are responsible for triggering public rights complaints following penal and administrative procedures, and for supervising and executing the provisions of the law; however, the competent court has a wide range of references in terms of the adaption and estimation of the actual damage, and in determining compensation and punishment.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Personal data can be processed directly, without the consent of the data subject, if the data is deemed necessary for the prevention or detection of crime. This interpretation is based on a judicial decision or an order of the prosecutor, and must be carried out to fulfil the aim of preventing, detecting or pursuing crimes committed contrary to the provisions of the law. This exception may also be used when necessary to protect the interests of the data subject regarding his or her personal data in relation to issues of life, death or vital interests, so long as this is done in a way that does not violate the provisions of the law, or when the personal data is directly accessible to the public.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

According to the law, all cookies targeting a data subject must be simple, clear, unambiguous and easy to access. Any consent required from the data subject must be clear and affirmative.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

According to article 3/a/14, the proposed bill to protect PI (the Bill) restricts the sharing of personal information for marketing, except when prior consent has been obtained from the data subject.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no official rules or guidance relating to behavioural advertising; however, the Bill restricts the processing of data or taking any action that would make the data available to the public.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The Bill defines 'sensitive data' as information that can be used to identify an individual, including:

- ethnic origin or political opinions;
- religious beliefs;
- health-related data;
- data concerning criminal records; or
- genetic data or biometric data that may be processed to identify a human being.

According to article a/11, the Bill does not authorise the processing of any sensitive information without the appointment of a data officer to monitor the process.

Profiling

44 | Are there any rules regarding individual profiling?

Article 5/b/4 of the Bill regulates the process of automated processing on personal information, granting individuals the right to oppose profiling that is unnecessary or exceeds the limit of the purpose for which the data had been compiled. However, individual profiling may be used without prior consent when necessary for medical or preventive purposes.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

A government cloud policy was passed in 2020, which governs cloud computing services.

NSAIR & PARTNERS
LAWYERS

Ma'in Nsair
main@nsairs.com

Haya Al-Erqsousi
h.alerqsousi@nsairs.com

Mariana Abu-Dayah
m.abudayah@nsairs.com

Odai Oqlat
o.oqlat@nsairs.com

362 Wasfi Al-Tal St. Dabouq
4th Floor, Office no. 405
P.O. Box: 962596
Amman 11196
Jordan

Tel: +962 7 77613336
Fax: +962 6 5660902
info@nsairs.com
www.nsairs.com

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Currently, Jordan does not have a data protection law. As a consequence, both the government and the private sector in the country have been collecting and exploiting PI of individuals without their prior consent.

Owing to the lack of data protection, the Parliament of Jordan is currently working on new legislation to meet international standards. The draft bill for the Data Protection Law of 2022 (the Bill) has been under development for many years, having been first introduced in 2014. Although movement on the Bill is welcomed, serious doubts remain about its ability to protect the privacy of individuals.

There are many similarities between the EU General Data Protection Regulation and previous PI legislation, but there are also many weaknesses that undermine the Jordanian legislation's effectiveness. One such issue is the proposed structure of the new data protection authority, which has raised concerns in civil society in Jordan. Specifically, the authorities would be chaired by the Ministry of Digital Economy and Entrepreneurship, which means that the government may be able to interfere in the modus operandi of the data protection authorities. This issue is exacerbated by the fact that more than one authority will be formed by the Bill, potentially leading to overlapping with the remits of these bodies.

Malaysia

Jillian Chia Yan Ping, Natalie Lim, Beatrice Yew and Nicole Oh Jia Yi
SKRINE

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Personal Data Protection Act 2010 (PDPA), which is based on data protection principles akin to those found in the EU Data Protection Directive 95/46/EC (the General Data Protection Regulation), came into force on 15 November 2013. The following subsidiary legislations have since been enacted under the PDPA:

- the Personal Data Protection Regulations 2013;
- the Personal Data Protection (Class of Data Users) Order 2013;
- the Personal Data Protection (Registration of Data User) Regulations 2013;
- the Personal Data Protection (Fees) Regulations 2013;
- the Personal Data Protection (Compounding of Offence) Regulations 2016; and
- the Personal Data Protection (Appeal Tribunal) Regulations 2021.

The Personal Data Protection Standard 2015 (PDP Standard) also sets out the minimum standards to be observed by data users when handling personal data and the enforceable codes of practice for the following sectors have been registered:

- the utilities sector (electricity);
- the insurance or takaful industry;
- the banking and financial sector;
- the transportation sector (aviation);
- the communications sector;
- the utilities sector (water); and
- the private hospitals in the healthcare industry.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

As the responsible authority in Malaysia, the functions of the Personal Data Protection Commissioner (the Commissioner) include advising the Minister of Communications and Multimedia on the national data protection policy and implementing and enforcing data protection laws.

The Commissioner has the power to do all things necessary or expedient for or in connection with the performance of his or her functions under the PDPA. This includes the power to investigate (such as where the Commissioner has reasonable grounds to believe that the PDPA has been breached or is being breached or where a proper complaint has been lodged), inspect a data user's personal data system, access computerised data, and search and seize with or without warrant.

The Commissioner may also serve an enforcement notice upon investigation, which specifies the breach, remedial steps required and the deadline for compliance or, if necessary, direct the data user to cease processing.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The PDPA provides that it is a function of the Commissioner to liaise and cooperate with persons performing similar personal data protection functions in any place outside Malaysia in respect of matters of mutual interest, including matters concerning the privacy of individuals concerning their personal data.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection law can lead to administrative sanctions and criminal penalties.

Depending on the nature of the offence, contravening the PDPA may lead to a fine between 100,000 ringgit and 500,000 ringgit and imprisonment of one to three years, although certain offences are compoundable, which may allow reduced penalties.

A breach of the PDPA may result in an inquiry or investigation by the Commissioner (either on its own initiative or based on a complaint received). Where following the investigation, the Commissioner decides that the PDPA has been contravened, the Commissioner may serve an enforcement notice, specifying the breach, the steps required to be taken to remedy the breach within a certain period and directing, if necessary, the relevant data user to cease processing the personal data. Fines of up to 200,000 ringgit or two years' imprisonment or both are possible for failure to comply with the Commissioner's enforcement notice.

Generally, a breach of any of the seven data protection principles may incur a fine of up to 300,000 ringgit and two years' imprisonment.

The Commissioner may also revoke the registration of a data user in certain circumstances, (eg, if the data user has failed to comply with the provisions of the PDPA or with any conditions imposed as part of the registration).

If a business commits an offence, its directors, chief executive officers, chief operating officers and other similar officers may be charged severally or jointly for non-compliance by the business, subject to certain limited defences.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Data users aggrieved by the Commissioner's decision may appeal to the Personal Data Protection Appeal Tribunal. The decisions that may be appealed are:

- decisions relating to the registration of data users;
- refusal of the Commissioner to register a code of practice;
- service of an enforcement notice;
- the Commissioner's refusal to vary or cancel an enforcement notice; and
- the Commissioner's refusal to conduct or continue an investigation based on a complaint.

If unsatisfied with the Personal Data Protection Appeal Tribunal's decision, the data user may file a judicial review in the Malaysian High Courts.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data Protection Act 2010 (PDPA) governs personally identifiable data that is processed in respect of a 'commercial transaction' but certain sectors and types of processing are exempted, such as:

- the processing of information for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010; and
- the processing of information by the Malaysian federal and state governments.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

There are no express provisions on interception of communications or monitoring and surveillance of individuals under the PDPA but to the extent that it involves the processing of personal data in respect of commercial transactions, the PDPA would apply. Electronic marketing is also subject to the PDPA and on marketing, the PDPA does give the individual the right to require a data user to cease or not to begin processing his or her personal data for the purposes of 'direct marketing' (communication by any means that is directed to particular individuals).

The telecommunications and computer crimes laws also generally prohibit the unlawful interception of communications or unauthorised access or use or interception of any computer or device. Electronic marketing must also not be done in a way that may contravene our telecommunications law that prohibits communications initiated to annoy, abuse, threaten or harass a person.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Various laws apply depending on the specific type of data. Below are just some examples of laws that apply to financial and health data.

The Financial Services Act 2013 (FSA) prohibits the disclosure of any document or information relating to the affairs or account of a customer of a financial institution to another person except in certain permitted circumstances. The Central Bank of Malaysia has also issued the Guidelines on Data Management and MIS Framework (the BNM Guidelines) to govern data management by the financial sector. The BNM Guidelines applies to all the institutions licensed under the FSA and all the institutions licensed under the Islamic Financial Services Act 2013.

The Private Healthcare Facilities and Services (Private Medical Clinics or Private Dental Clinics) Regulations 2006 also govern the processing, management and retention of patients' medical records and the processing of healthcare information is also governed by certain confidentiality guidelines issued by the Malaysian Medical Council.

PI formats

9 | What categories and types of PI are covered by the law?

Any information relating directly or indirectly to an individual who is identified or identifiable from that information or from that and other information in the data user's possession is considered personal data within the ambit of the PDPA. This includes 'sensitive personal data', which includes information relating to mental or physical health, political opinions, religious beliefs and other beliefs of a similar kind as well as information relating to the commission or alleged commission of any offence or any other personal data as the Minister of Communications and Multimedia may determine by a gazette order. Such broad definition includes data in electronic and manual form.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The PDPA applies to data users who are:

- established in Malaysia (and the personal data is processed by that person or any other person employed or engaged by that establishment); or
- not established in Malaysia, but use equipment in Malaysia to process the personal data otherwise than for the purposes of transit through Malaysia.

The PDPA will not apply to any personal data processed outside Malaysia unless it is intended to be further processed in Malaysia.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

'Processing' is defined widely to include collection, recording, storage and use of personal data, but the PDPA applies to personal data processed in respect of a commercial transaction only. Certain types of processing are also exempted (eg, processing by an individual only for his or her personal, family or household affairs is exempted).

The PDPA distinguishes between a 'data user', 'data processor' and 'data subject'. A data user, which is conceptually similar to a controller, means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data but does not include a processor. A data processor means any person other than an employee of the data user who processes personal data solely on behalf of the data user and does not process the personal data for any of his or her own purposes. The obligations are imposed on the data user and there are specific obligations imposed on the data user where a data processor is used. However, the data processor is not bound directly under the PDPA.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Personal Data Protection Act 2010 (PDPA) requires consent (for processing of non-sensitive personal data) and explicit consent (for processing of sensitive personal data), failing which the processing must be legitimised on specific grounds for exemptions. For non-sensitive personal data, the PDPA provides certain exemptions where the processing is necessary:

- for the performance of a contract to which the individual is a party;
- for the taking of steps at the request of the individual to enter into a contract;
- for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
- to protect the individual's vital interests;
- for the administration of justice; or
- for the exercise of any functions conferred on any person by or under any law.

Processing sensitive personal data without explicit consent is subject to separate exemptions.

But there are conditions for processing that the data user must comply with (regardless of whether consent or explicit consent has been obtained). Personal data must not be processed unless:

- the personal data is processed for a lawful purpose directly related to an activity of the data user;
- the processing of the personal data is necessary for or directly related to that purpose; and
- the personal data is adequate but not excessive concerning that purpose.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

Stricter rules apply to the processing of 'sensitive personal data', which includes information relating to mental or physical health, political opinions, religious beliefs and other beliefs of a similar kind as well as information relating to the commission or alleged commission of any offence or any other personal data as the Minister of Communications and Multimedia may determine by a gazette order. Processing sensitive personal data requires explicit consent unless an exemption applies. Some examples are where the processing relates to information that has been made public as a result of steps deliberately taken by the data subject or where the processing is necessary:

- to exercise or perform any right or obligation that is conferred or imposed by law on the data user in connection with employment;
- to protect the vital interests of the data subject or another person, where consent cannot be given by or on behalf of the data subject or the data user cannot reasonably be expected to obtain the consent of the data subject;
- to protect the vital interests of another person, where consent by or on behalf of the data subject has been unreasonably withheld; or
- to obtain legal advice, or the establishment, exercising or defence of legal claims.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

A data user must inform the individual in writing in English and Malay of the following:

1 that the individual's personal data is being processed by or on behalf of the data user, with a description of the personal data;
2 the purposes for which the personal data is being or is to be collected and further processed;
3 of any information available to the data user as to the source of that personal data;
4 of the individual's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;
5 of the class of third parties to whom the data user discloses or may disclose the personal data;
6 of the choices and means the data user offers the individual for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
7 whether it is obligatory or voluntary for the individual to supply the personal data; and
8 where obligatory, the consequences of failure to supply the personal data.

In relation to (4) above, the Personal Data Protection Regulations 2013 provide that the data user must at least provide the data subject with the following details:

- designation of the contact person;
- phone number;
- fax number, if any;
- email address, if any; and
- such other related information.

The notice must also be given 'as soon as practicable' when:

- the individual is first asked by the data user to provide his personal data;
- when the data user first collects the personal data; or
- in any other case before the data user uses the personal data for a purpose other than the purpose for which the personal data was collected or before the data user discloses the personal data to a third party.

The Personal Data Protection Department recently issued the Guide to Prepare Personal Data Protection Notice (the Guide), which requires the following additional information or 'compulsory elements' to be stated in personal data protection notices:

- any sensitive personal data involved in processing;
- if personal data of children under 18 years old is processed;
- if there is any regulator requirement to collect certain personal data;
- how long the personal data will be retained in such processing;
- when the personal data be will disposed of;
- what practical measures will be taken to ensure personal data is secured;
- name of the person in charge in relation to how to contact data user for queries or complaints regarding personal data;
- the names of third parties to whom the personal data of data subject are shared with and for what purpose; and

- the security measures in place to ensure the disclosure implemented is safe and secure.

It remains uncertain at present whether the Guide is legally binding.

Exemptions from transparency obligations

15 | When is notice not required?

Notice is not required when personal data:

- is processed for the prevention or detection of crime or the purpose of investigations, apprehension or prosecution of offenders, or assessment or collection of any tax or duty or other similar impositions;
- is processed to prepare statistics or carry out research provided that the resulting statistics or research results are not in a form that identifies the individual;
- is necessary for or in connection with any court judgment or order;
- is processed to discharge regulatory functions if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; and
- is processed for journalistic, literary or artistic purposes, provided that the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material, the publication would be in the public interest and compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Data users must take reasonable steps to ensure the personal data is accurate, complete, not misleading and kept up to date, having regard to the purpose (and any directly related purpose) for which it was collected and processed. Data users must also comply with the data integrity standards set by the Personal Data Protection Commissioner (the Commissioner) (eg, the data user must update the personal data immediately upon receiving a data correction notice from the individual and notify the individual of the update through appropriate methods).

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The Personal Data Protection Act 2010 (PDPA) does not restrict the types or volume of PI that may be collected, but the General Principle in the PDPA prescribes that personal data must not be processed unless the personal data is adequate but not excessive in relation to the purpose for which it is processed.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Personal data cannot be kept longer than is necessary to fulfil the processing purpose unless a longer retention period is required by law (eg, Malaysian tax laws generally require all relevant records and documents to be retained for seven years). Retention must be in accordance with the retention standards set by the Commissioner, which further specify the time frame (eg, the data user must dispose of any personal data collection forms used for commercial transactions within 14 days, unless they carry legal value in relation to the commercial transaction).

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

There are no express restrictions on the purposes for which PI can be used in the PDPA, but there are similar conditions of processing under the General Principle, where data users may not process personal data unless it is for a lawful purpose directly related to the data user's activity, the processing is necessary and directly related to the purpose, and the personal data is adequate and not excessive concerning that purpose. Processing must also be restricted to the purposes described in the notice.

For new purposes, consent must be obtained again unless any of the exceptions to the consent requirement apply. The notice must also be amended to cater to the new purpose.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The PDPA does not currently contain any requirements or restrictions relating to automated decision-making.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Data users must 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 nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;
- to the place or location where the personal data is stored;
- to any security measures incorporated into any equipment in which the personal data is stored;
- to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
- to the measures taken for ensuring the secure transfer of the personal data.

If the processing is carried out by a data processor on behalf of a data user, the data user must ensure that the data processor:

- provides sufficient guarantees in respect of the technical and organisational security measures governing the processing; and
- takes reasonable steps to ensure compliance with those measures.

The data user must develop and implement a security policy that must be compliant with the Personal Data Protection Act 2010 (PDPA) and the security standards set by the Personal Data Protection Commissioner (the Commissioner). The following is a brief non-comprehensive overview of the prescribed security standards.

In respect of electronically processed personal data:

- to ensure personnel who manage personal data are registered under a registration system before being granted access to personal data and to provide a user ID and password to staff given access to the personal data;

- to control and limit the authority of staff to access personal data for purposes of collection, processing and retention of the personal data;
- to ensure all staff involved in the processing of personal data always protects the confidentiality of personal data;
- to implement physical security procedures such as entry and exit controls, storage of personal data in locations that are safe from physical or natural threats and not exposed, installation of close circuit television around data storage areas (if required), and 24-hour security of facilities (if required);
- to implement backup and recovery systems;
- the latest antivirus software must be deployed and scheduled malware monitoring and scanning of operating systems to prevent attacks on electronically stored data must be implemented; and
- to maintain proper access records to personal data periodically, which must be presented when instructed by the Commissioner.

In respect of non-electronically processed personal data:

- to prescribe physical security procedures such as:
  - to keep all personal data properly in a file;
  - keep all files containing personal data in a locked area;
  - keep all relevant keys in a safe place;
  - keep a record of key storage; and
  - to store personal data in an appropriate location;
- the transfer of personal data using conventional methods such as through post, by hand, fax or others must be recorded;
- to ensure that all used paper, printed documents or other documents that clearly shows personal data must be properly destroyed; and
- conduct awareness programmes on the responsibility to protect personal data for all relevant personnel (if necessary).

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The PDPA does not currently provide for this and does not define 'data breach', but the authorities issued a public consultation paper in 2018, The Implementation of Data Breach Notification, which sought to introduce a data breach notification regime, where data users would be required to notify regulators and affected individuals in the event of a data breach. The consultation paper sets out, among other things:

- the requirement to notify the Commissioner within 72 hours of becoming aware of the data breach incident and to provide details about the data at risk;
- actions that have been taken or will be taken to mitigate the risks to the data;
- details of notifications to affected individuals; and
- details of the organisation's training programmes on data protection.

However, the consultation paper has yet to be gazetted as law.

While it is not a mandatory requirement under the PDPA, an online data breach notification to the Commissioner can be made. The required information includes:

- the particulars of the data user and the person giving the notification;
- the details of the data breach;
- containment and recovery; and
- notifications made to other parties (regulators and law enforcement agencies, affected parties, data processors, or other overseas data protection authorities).

Under this voluntary data breach notification regime, the data breach incident should be reported within 72 hours.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The Personal Data Protection Act 2010 (PDPA) does not have express accountability principles per se, but data users are required to develop and implement a security policy which is compliant with the security standards set by the Personal Data Protection Commissioner (the Commissioner).

To demonstrate compliance with the law, a data user must keep and maintain a record of any application, notice, request or any other information relating to personal data processed by him in the form and manner that may be determined by the Commissioner. The personal data system must also be open for inspection, and the Commissioner or inspection officer may require certain documents to be produced including, inter alia, record of consent and notice, list of disclosures to third parties and the security policy.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The PDPA does not presently mandate the appointment of a data protection officer.

However, pursuant to the Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010, dated 14 February 2020, the Commissioner is considering introducing an obligation in the PDPA for a data user to appoint a data protection officer and introduce a guideline pertaining to officers.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

A data user must keep and maintain a record of any application, notice, request or any other information relating to personal data processed by him or her in the form and manner that may be determined by the Commissioner.

The personal data system must also be open for inspection, and the Commissioner or inspection officer may require certain documents to be produced, including records of consent and notices, a list of disclosures to third parties and the security policies. Other laws may also prescribe record-keeping requirements (eg, tax laws).

Risk assessment

26 Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

PDPA does not presently require data users to carry out risk assessments.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The PDPA does not presently require data users to apply a privacy-by-design or privacy-by-default approach. However, pursuant to the Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010, dated 14 February 2020, the Commissioner is considering a proposal to instruct that any new system is required to apply privacy by design and to issue a guideline on the mechanism.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There are no exemptions for registration for data users but only data users falling within the class of data users prescribed in the Personal Data Protection (Class of Data Users) Order 2013, which are largely limited to licensees within a particular sector, must register with the Personal Data Protection Commissioner (the Commissioner). The sectors are:

- communications;
- banking and financial institutions;
- insurance;
- health;
- tourism and hospitality industries;
- transportation;
- education;
- direct selling;
- services (legal, audit, accountancy, engineering or architecture);
- real estate;
- utilities;
- pawnbrokers; and
- moneylenders.

Applications for registration can be done online and a registration fee is payable. Information required includes, inter alia, the name and information of the company and information of the person in charge of the registration. The documents required include, inter alia, incorporation documents and relevant licences. Any document as may be required by the Commissioner must also be submitted. Registration certificates are valid for at least one year, after which data users must renew registrations.

Data users falling under a prescribed class of data users required to register who process personal data without a registration certificate commit an offence and may be liable to a fine of up to 500,000 ringgit or imprisonment for up to three years, or both.

Other transparency duties

29 | Are there any other public transparency duties?

Not applicable.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Persons other than the data user's employee who process personal data solely on the data user's behalf and not for their own purposes are considered 'data processors'.

In respect of data processors, data users must ensure that:

- data processors provide sufficient guarantees in respect of the technical and organisational security measures governing the processing; and
- reasonable steps are taken to ensure compliance with those measures, (eg, ensure constant monitoring in respect of the data processors' compliance with their guarantees).

The security standards set by the Personal Data Protection Commissioner (the Commissioner) also require a contract to be established between a data user and the data processor. The security standards also prescribe certain security measures for electronic transfers. If the outsourcing involves the cross-border transfer of personal data, the Personal Data Protection Act 2010 (PDPA) prohibits such transfer except in certain circumstances (eg, consent has been obtained, the transfer is necessary for the performance of a contract between the data subject and the data user, or the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA (among other exceptions)). Other laws may impose further restrictions (eg, disclosure of banking account-related data is prohibited by Malaysian financial laws except in certain permitted circumstances).

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

A data user cannot disclose personal data without the individual's consent unless it is for the purpose it was collected for or if the disclosure is to a third party that was specified in the notice to the data subject. A list of third-party disclosure must also be maintained.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Cross-border transfer of personal data is prohibited unless it is to a gazetted place. Public Consultation Paper No. 1/2017 on the Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 proposing the whitelisted countries has been issued but no country has yet to be gazetted as a permitted country.

Notwithstanding the prohibition, cross-border transfers are permissible in certain specified circumstances, among others:

- the individual's consent has been obtained;
- the transfer is necessary for the performance of a contract between the individual and the data user;
- the data user has taken all reasonable steps and exercised all due diligence to ensure the personal data will not be processed in a manner that would contravene the PDPA;
- the transfer is necessary for legal proceedings or to obtain legal advice; and
- the transfer is necessary to protect the individual's vital interest and for the public's interest.

There are presently no supervisory authority notification or authorisation requirements for cross-border data transfers under the PDPA.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The PDPA does not distinguish between transfers to service providers and onwards transfer. The restrictions apply equally to both types of transfers.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no general data localisation requirements under the PDPA. However, there may be other laws or industry-specific rules that require this (eg, there may be requirements under tax and company law to maintain certain accounting reports and records relating to any business in Malaysia locally, as well as industry-specific laws to keep data within Malaysia, particularly in the financial services sector).

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Access Principle, a data subject has a right of access to his or her data and to correct it if it is inaccurate, incomplete, misleading or outdated.

Certain prescribed procedures have been set out where access or correction is requested by the data subject (ie, where the data subject requires a copy of the personal data, the data user must acknowledge receipt of the request). The Personal Data Protection Regulations 2013 also set out the information that may be requested by a data user when processing an access request.

Generally, a data user must comply with an individual's request to access and correct their personal data, except where:

- the data user is not supplied with sufficient information as to the identity of the requestor or of the relevant person making the request (information that may be requested includes identification card number and address);
- the data user is not supplied with sufficient information to enable him or her to locate the personal data;
- the burden or expense of providing access is not proportionate to the risk of the data subject's privacy;
- the data user cannot comply with the request without disclosing the personal data of another individual who is identifiable from that information (unless consent of that individual has been obtained or it is reasonable to comply without the consent of such other individual);
- the processing of personal data is controlled by another data user in a manner that prohibits the relevant data user from complying in whole or part with the request;
- it will be against any court order;
- it will disclose confidential commercial information; or
- the access is regulated by another law.

Other rights

36 | Do individuals have other substantive rights?

The Personal Data Protection Act (PDPA) also confers the following rights on the individuals:

- the right to withdraw consent to process personal data;
- the right to prevent processing likely to cause damage or distress; and
- the right to prevent processing for direct marketing.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The PDPA does not give individuals the right to pursue civil claims against data users for breaching the PDPA.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Not applicable.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Not applicable.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The Personal Data Protection Act 2010 (PDPA) does not have specific provisions on cookies or equivalent technology but such processing is subject to the PDPA's general provisions assuming the information collected contains personal data.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

Under the PDPA, an individual has the right to require a data user to cease or not begin processing his or her personal data for direct marketing purposes. The definition of 'direct marketing' is broad enough to cover marketing by email, fax or telephone.

Marketing messages electronically transmitted are also governed by Malaysia's telecommunications law. There are no specific provisions on the illegality of 'spam', but section 233(1)(b) of the Communications and Multimedia Act 1998 (CMA) provides that:

> *[A] person who initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address commits an offence.*

The Malaysian Communications and Multimedia Commission (MCMC) acknowledges that this provision may be inadequate in dealing with spam, but it should be ensured the marketing messages are not sent in a manner that contravenes this prohibition, (eg, sending messages repeatedly and continuously such that the intent to annoy, abuse, etc, could be implied).

The MCMC also issued guidance on spamming, including:

- the public consultation report on Regulating Unsolicited Commercial Messages, dated 17 February 2004;
- FAQs on the MCMC website; and
- the Anti-Spam Toolkit, which contains the Anti-Spam Framework of Best Practices and Technical Guidelines.

Generally, the main distinguishing factor between a legitimate message and spam is consent. The marketer must obtain the recipient's permission or consent before sending out marketing messages and the target audience should be those who have expressed an interest in a particular product or service being marketed by that sender. Whether the anti-spam rules are legally binding is unclear, but compliance would be good practice.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are presently no specific rules on targeted online advertising under the PDPA.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Stricter rules apply to processing of 'sensitive personal data', which includes information relating to mental or physical health, political opinions, religious beliefs and other beliefs of a similar kind, as well as information relating to the commission or alleged commission of any offence or any other personal data as the Minister of Communications and Multimedia may determine by a gazette order. Processing sensitive personal data requires explicit consent unless an exemption applies. Some examples are where the processing relates to information that has been made public as a result of steps deliberately taken by the data subject or where the processing is necessary:

- for the purposes of exercising or performing any right or obligation that is conferred or imposed by law on the data user in connection with employment;
- to protect the vital interests of the data subject or another person, where consent cannot be given by or on behalf of the data subject or the data user cannot reasonably be expected to obtain the consent of the data subject;
- to protect the vital interests of another person, where consent by or on behalf of the data subject has been unreasonably withheld; or
- for the purposes of obtaining legal advice, or the establishment or exercise of defence of legal claims.

Profiling

44 | Are there any rules regarding individual profiling?

There are presently no specific rules on individual profiling under the PDPA.

SKRINE

Jillian Chia Yan Ping
jc@skrine.com

Natalie Lim
natalie.lim@skrine.com

Beatrice Yew
beatrice.yew@skrine.com

Nicole Oh Jia Yi
nicole.oh@skrine.com

Level 8, Wisma UOA Damansara
50 Jalan Dungun, Damansara Heights
50490 Kuala Lumpur
Malaysia
Tel: +60 3 2081 3999
www.skrine.com

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The use of cloud computing services is subject to the PDPA's general requirements, but the following security standards set by the Personal Data Protection Commissioner relate specifically to cloud services:

- the transfer of personal data using removable media device and cloud computing service is not allowed except with the written approval of an authorised officer from the upper management of the data user's organisation;
- the transfer of personal data using removable media devices and cloud computing services must be recorded; and
- that the transfer of personal data using cloud computing service must follow the personal data protection principles in Malaysia and other countries with personal data protection laws.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Personal Data Protection Commissioner issued a proposal paper, Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 (PC01/2020), dated 14 February 2020, to seek the views and comments of the public as part of an ongoing review of the Personal Data Protection Act 2010. Some of the issues for which feedback is sought include the extension of obligations to data processors, data portability, the appointment of a data protection officer, the reporting of data breaches and providing the right to commence civil litigation against data users.

Malta

Paul Gonzi and Sarah Cannataci
Fenech & Fenech Advocates

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The primary national legislative instrument regulating the protection of PI in Malta is the Data Protection Act (the Act), Act XX of 2018 as amended by Act XII of 2021 (Chapter 586 of the Laws of Malta) and subsidiary legislation issued thereunder. The full title of the Act is 'An Act to repeal and to replace the Data Protection Act, Cap 440'. Chapter 440 remains in force solely for any breach that occurred before the Act came into force.

Maltese legislation regarding data protection matters transposes and implements various EU directives and regulations, most notably:

- Regulation (EU) 2016/679 on the protection of natural persons concerning the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR);
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector;
- Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services; and
- Directive 2002/58/EC and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

Maltese legislation is also in conformity with the Convention of the Council of Europe for the Protection of Individuals concerning Automatic Processing of Personal Data (ETS NO 108), which was ratified by Malta in February 2003.

Under the European Convention Act (Chapter 319 of the Laws of Malta), the European Convention on Human Rights, including the protection afforded in respect of the right to privacy (article 8), has been transposed into domestic Maltese law and is directly enforceable before the Maltese courts. The right to privacy of one's home and property as well as the right to freedom of expression are enshrined in the Constitution of Malta as fundamental human rights.

Further, the EU Charter of Fundamental Rights, which recognises the right to privacy and the right to data protection, applies to national authorities when implementing EU law.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Act establishes the Information and Data Protection Commissioner (the Commissioner or IDPC), who heads an independent regulatory authority overseeing all aspects of data protection.

The IDPC has the power to:

- institute civil judicial proceedings in cases where the provisions of the Act or the GDPR have been or about to be violated;
- seek the advice of, and consult with, any other competent authority in the exercise of its functions under the Act and the GDPR;
- request the assistance of the executive police to enter and search any premises in the exercise of the investigative powers under article 58 of the GDPR;
- confer powers, including investigative powers, on the seconding supervisory authority's members or staff, in the case of joint operations with supervisory authorities of one or more other EU member states; and
- impose administrative fines.

Decisions of the Commissioner are subject to appeal before the Information and Data Protection Appeals Tribunal, and decisions of the Tribunal are also subject to review before the Court of Appeal.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Act establishes that the IDPC may seek the advice of, and may consult with, any other competent authority in the exercise of his or her functions and that in the event of joint operations with supervisory authorities of one or more other EU member states, may confer powers, including investigative powers, on the seconding supervisory authority provided the powers are exercised under the guidance and in the presence of the IDPC.

Under the GDPR, the IDPC must cooperate on cases with a cross-border component to ensure a consistent application of the GDPR – this being the one-stop-shop mechanism.

In the context of the processing of PI in the electronic communications sector, the IDPC is also empowered to seek the advice of, and where appropriate must consult with, the Malta Communications Authority in the exercise of its functions.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection law can lead to the imposition of administrative fines by the IDPC, which are capped for public authorities or bodies and vary depending on which obligations at law have been infringed.

In this regard, any administrative fines imposed are due to the IDPC as a civil debt, and therefore the IDPC can take civil action to recover this debt.

Also, the provision of false information to the IDPC or non-compliance with any lawful request pursuant to an investigation by the IDPC is an offence and shall, upon conviction, be liable to a criminal fine or imprisonment or both. Other than for these offences, a breach of data protection legislation shall not give rise to criminal liability, unless the act or omission gives rise to another criminal offence, such as that of computer misuse regulated by the Criminal Code, Chapter 9 of the Laws of Malta.

Judicial review of data protection authority orders

5 Can PI owners appeal to the courts against orders of the data protection authority?

The Information and Data Protection Appeals Tribunal (the Tribunal) is established under the Data Protection Act to hear appeals from the decisions of the Commissioner in its role as the supervisory authority. Any party to the appeal may appeal the decision of the Tribunal to the Court of Appeal on a point of law.

Separately, data subjects may institute an action for effective judicial remedy, as well as an action for damages (including moral damages), against a data controller or processor before the First Hall of the Civil Court. Such a decision is also subject to appeal.

SCOPE

Exempt sectors and institutions

6 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Data Protection Act (the Act) applies to:

- the processing of PI in the context of the activities of an establishment of a controller or a processor in Malta or a Maltese Embassy or High Commission abroad, regardless of whether the processing takes place in Malta or not;
- the processing of PI of data subjects who are in Malta by a controller or processor not established in the European Union, where the processing activities are related to:
    - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Malta; or
    - the monitoring of their behaviour in so far as their behaviour takes place within Malta; and
- the processing of PI by a controller not established in the Union but in a place where the laws of Malta apply under public international law.

The processing of PI in the course of an activity that falls outside the scope of EU law, or by the Maltese government when carrying out activities that fall within the scope of Chapter 2 of Title V of the Treaty on European Union, fall outside of the scope of the Act.

Processing of PI by a natural person in the course of a purely personal or household activity is also excluded, as is also the processing of PI by competent authorities in the area of crime prevention and prosecution. In the latter case, the Data Protection (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) Regulations (Subsidiary Legislation No. 586.08) applies.

Further to article 23 of Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR), Subsidiary Legislation No. 586.09 (the Restriction of the Data Protection (Obligations and Rights) Regulations) was enacted to regulate restrictions to certain data subject rights and obligations arising under the GDPR.

Interception of communications and surveillance laws

7 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation No. 586.01), as subsidiary legislation of the Act, regulates the processing of PI in connection with the provision of publicly available electronic communications services in public communications networks in Malta and any other country, including public communications networks supporting data collection and identification devices.

The Regulations include provisions on the interception and surveillance of communications and traffic data, as well as on the limitations on the storing of information or gaining of access to information stored in data terminal equipment, such as by the use of web cookies. They also make provision for the monitoring of traffic data and location data.

The Regulations also provide for the conditions required to be satisfied for lawful electronic marketing and the limitation on unsolicited communications in the context of direct marketing, as well as the exception applicable to customers.

The monitoring and surveillance of individuals is also regulated under the GDPR, the Act and other subsidiary laws.

Other laws

8 Are there any further laws or regulations that provide specific data protection rules for related areas?

Further laws or regulations that provide specific data protection rules for related areas include:

- Subsidiary Legislation No. 586.04, Processing of Personal Data (Protection of Minors) Regulations;
- Subsidiary Legislation No. 586.06, Processing of Personal Data for the purposes of the General Elections Act and the Local Councils Act Regulations;
- Subsidiary Legislation No. 586.07, Processing of Personal Data (Education Sector) Regulations;
- Subsidiary Legislation No. 586.08, Data Protection (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) Regulations;
- Subsidiary Legislation No. 586.09, Restriction of the Data Protection (Obligations and Rights) Regulations;
- Subsidiary Legislation No. 586.10, Processing of Data concerning Health for Insurance Purposes Regulations;
- Subsidiary Legislation No. 586.11, Processing of Child's Personal Data in relation to the Offer of Information Society Services Regulations;
- the Criminal Code (Chapter 9 of the Laws of Malta), Title IX, Cooperation between the National Authorities and the Office of the European Public Prosecutor;

- Identity Card and Other Identity Documents (Chapter 258 of the Laws of Malta), on the limitations of the use of biometric data stored on an electronic identity card;
- the Accountancy Profession Act (Chapter 281 of the Laws of Malta), on the remit and limitations of the Accountancy Board;
- the Income Tax Management Act (Chapter 372 of the Laws of Malta), on the partial or complete restriction of data subject rights, in particular, the right of access, and on the limitations of the Commissioner of Inland Revenue to request special category data;
- Subsidiary Legislation No. 378.10, Credit Agreements for Consumers relating to Residential Immovable Property Regulations on the limitations of processing of personal data obtained from a consumer or any other person in connection with the conclusion and management of any credit agreement, in so far as this may only be processed for the purpose of assessing the consumer's creditworthiness or of any such other person and their ability to repay in accordance with these regulations;
- Subsidiary Legislation No. 399.48, Part VIII of the Electronic Communications Networks And Services (General) Regulations on the protection of privacy, which regulate, among others, calling-line identification;
- Subsidiary Legislation No. 424.34, the Work Place (Minimum Health and Safety Requirements for the Protection of Workers from Risks resulting from Exposure to Electromagnetic Fields) Regulations on the limitations on the right of access in the context of safety risk assessments;
- Subsidiary Legislation No. 427.101, the Olive Oil (Marketing Standards) (Implementing) Regulations. Establishing a public interest ground for the sharing of data and information by persons, natural or legal, for the purposes of the Director General's functions;
- Subsidiary Legislation No. 452.104, the Telework National Standard Order, on measures, particularly concerning software, that employers of teleworkers must implement to ensure the protection of data used and processed by the teleworker in the carrying out of duties;
- Subsidiary Legislation No. 458.43, the Clinical Trials Regulations on the rules regulating clinical trials, including assurances on the rights of the subject to physical and mental integrity, to provide and protection of data concerning him or her;
- Subsidiary Legislation No. 460.18, the Communication of Passenger Data by Air or Sea Carriers Order on the rules regulating the processing of personal data by the Principal Immigration Officer, including on retention periods;
- the Securitisation Act (Chapter 484 Laws of Malta), on the transfer of transfers of personal data, including to third countries without adequate levels of protection, within the context of securitisation transactions;
- the Voluntary Organisations Act (Chapter 492 of the Laws of Malta), on disclosures of personal data processed by the Commissioner for Voluntary Organisations;
- Subsidiary Legislation No. 499.61, the Deployment and Use of Intelligent Transport Systems Regulations on the processing of personal data in the context of Intelligent Transport Systems and the preference for anonymous data in the performance of ITS applications and services;
- Subsidiary Legislation No. 499.62, the Motor Vehicles(Exchange of Data) Regulations on, inter alia, retention periods of personal data processed by competent authorities;
- the Health Act (Chapter 528 of the Laws of Malta), on, inter alia, the limitation of the access right by a patient;
- Subsidiary Legislation No. 528.100, the Processing of Personal Data (Secondary Processing) (Health Sector) Regulations on, inter alia, secondary processing the processing of personal data and health records for research activities;
- Subsidiary Legislation No. 546.02, the Business Register and Information Sharing Regulations on the establishment of a business registry and inter alia, the rule that all undertakings listed thereon (including self-employed persons) are considered as business undertakings;
- the Coordination of Government Inspections Act (Chapter 568 of the Laws of Malta), which, inter alia, provides that the sharing of data, the maintenance of common databases and repositories of information, as provided for by this Act to facilitate reductions in the burden of inspections on entities and individuals, shall be regarded as activities that are carried out in the public interest for the purposes of the Data Protection Act;
- Subsidiary Legislation No. 583.09, the Gaming Commercial Communications Regulations on the limitation of the processing of personal data, unsolicited commercial communications, and commercial communications to self-excluded players by authorised persons offering licensable games or service providers collaborating with authorised persons; and
- the Passenger Name Record (Data) Act (Chapter 584 of the Laws of Malta), transposing Directive (EU) 2016/681 on the protection of personal data and the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

The Data Protection Act also includes:

- exceptions and derogations from certain provisions of the GDPR in the context of the processing of PI for scientific or historical research purposes or official statistics;
- an obligation for controllers to consult with (and obtain authorisation from) the Information and Data Protection Commissioner where it intends to process in the public interest, any genetic data, biometric data or data concerning health for statistical or research purposes, or special categories of data concerning the management of social care services and systems;
- limitations on the processing of identification documentation; and
- special rules in the context of journalism and freedom of expression and information.

PI formats

9 | What categories and types of PI are covered by the law?

The law applies to the processing of PI, wholly or partly, by automated means and to such processing other than by automated means where such PI forms part of a filing system or is intended to form part of a filing system.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The law applies to the processing of PI by a controller or processor established in Malta or a Maltese embassy or high commission abroad, regardless of whether the processing takes place in Malta or not, and also to a controller not established within the European Union but in a place where the laws of Malta apply under public international law.

Further, the law also applies to the processing of PI of data subjects who are in Malta by a controller or processor not established in the European Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Malta; or

- the monitoring of their behaviour in so far as their behaviour takes place within Malta.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The Act sets out that the definitions as contained within article 4 of the GDPR shall apply, meaning that the definitions of a 'data subject', 'controller', 'processor' and 'processing' as set out therein apply.

Different obligations apply depending on whether the individual or entity processing personal data is a 'controller' or 'joint controller' or a 'processor'.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Processing of PI is legitimate if one of the following applies:

- the data subject has given consent to the processing of his or her PI for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary to protect the vital interests of the data subject or another natural person;
- processing is necessary for the performance of a task carried out in the public interest or 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 that require protection of PI, in particular where the data subject is a child.

Other conditions must be satisfied to process certain categories of data, such as health data and data relating to criminal convictions.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

PI constituting special categories (ie, PI revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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) shall not be processed unless a specific ground provided for in Regulation (EU) 2016/679 (General Data Protection Regulation) is satisfied. Special rules apply to the processing of criminal conviction data, and of unique numbers that identify persons.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Controllers are obliged by law to provide information relating to the processing of PI to the individual to whom the PI relates in a concise, transparent, intelligible and easily accessible form, using clear and plain language at the time when the PI is obtained, where the PI was collected directly from the individual concerning whom the PI relates. This must include, among others, the purpose and legal ground for processing, the recipients of the data, information on cross-border, transfers of data and retention periods.

Where the PI was not collected directly from the individual concerning whom the PI relates, the controller is obliged to provide the following information in addition to the above:

- the categories of PI concerned; and
- from which source the PI originate, and if applicable, whether it came from publicly accessible sources.

The controller is obliged to provide this additional information no later than one month after obtaining the PI. Where the PI is to be used for communication with the individual, the controller is obliged to provide this information, at the latest, at the time of the first communication with the individual. Where the PI is to be disclosed to another recipient, the controller is obliged to provide this information, at the latest, when the PI is first disclosed.

Exemptions from transparency obligations

15 | When is notice not required?

The controller is not obliged to provide this notification on the processing of PI where the individual already has the information.

Also, where the controller has obtained the PI from a third party, the controller shall be exempt from providing this information to the individual where the provision of such information proves impossible or would involve a disproportionate effort, or in so far as the provision of the information is likely to render impossible or seriously impair the achievement of the objectives of that processing operation.

Another exemption applicable if the PI was not obtained from the data subject is that where the PI must remain confidential subject to an obligation of professional secrecy or the obtaining or disclosure of the provision of information is regulated by EU or EU member state law to which the controller is subject.

The Data Protection Act (the Act), Chapter 586 of the Laws of Malta, also sets out that the controllers shall be exempt from notification where the processing is carried out for journalistic purposes or the purposes of academic, artistic or literary expression.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Processing of PI must satisfy six data protection principles, which are cumulative and not alternative. One of these core data protection principles is that of accuracy, wherein PI processed shall be accurate and, where necessary, kept up to date.

Inaccurate PI must be erased or rectified without delay.

Additionally, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate,

the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

The Act provides an exemption from compliance with the accuracy principle where the processing is carried out for journalistic purposes or the purpose of academic, artistic or literary expression.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The processing of PI must satisfy six data protection principles, which are cumulative and not alternative. One of these core data protection principles is that of data minimisation, wherein PI processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which the PI is processed.

The Act provides an exemption from compliance with the data minimisation principle where the processing is carried out for journalistic purposes or for the purpose of academic, artistic or literary expression.

Additionally, the Act also sets out restrictions on the processing of identity documents, in that this processing can only occur where it is clearly justified, with regard to the purpose of the processing and (1) the importance of a secure identification or (2) any other valid reason as may be provided by law.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

PI must be kept in a form that permits identification of individuals for no longer than is necessary for the purposes for which the PI are processed.

Very often, the law does not provide an express limitation period, and it shall be for the controller of PI to be able to demonstrate that the retention period satisfies the criteria. However, some sector-specific laws provide for strict retention periods.

The Act sets out that the controllers shall be exempt from compliance with the accuracy principle where the processing is carried out for journalistic purposes or for the purposes of academic, artistic or literary expression.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI must be processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Processing of PI for purposes other than those for which the PI was initially collected should be allowed only where the processing is compatible with the purposes for which the PI were initially collected. In this regard, the controller shall assess whether another purpose can be deemed to be 'compatible', by taking into account:

- any link between that purpose and the purposes of the intended further processing;
- the context in which the PI has been collected;
- the nature of the PI;
- the consequences of the intended further processing for data subjects; and
- the existence of appropriate safeguards in both the original and intended further processing operations.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The law does not set out any restrictions on the use of PI for making automated decisions without human intervention, other than the obligation on the part of the controller to inform the data subject about the processing in question. The data subject is also granted the right to ask for any decisions to be taken by a human being in lieu of automated decision-making.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

PI owners and their service providers are obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The legal framework also sets out a non-exhaustive list of examples of measures that can be applied in this regard, such as the implementation of pseudonymisation and encryption of PI.

In addition, the law sets out that where new technologies are to be implemented or where the processing operation is likely to result in a high risk, a data privacy impact assessment (DPIA) may have to be carried out.

Depending on the nature of PI being processed, the controller or processor may also be required to appoint a data protection officer.

Ultimately, the controller must be able to demonstrate the efforts towards compliance, and therefore it is a requirement to have proper records that satisfy the principle of accountability. Certain controllers and processors are mandated to retain a minimum set of records, aside from standard policies and protocols that are expected to be maintained.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Unless a breach is unlikely to result in a risk to the rights and freedoms of natural persons, the controller is obliged to notify the breach within 72 hours of becoming aware of the same breach.

Where a processor has suffered a data breach, notification to the controller must be made without undue delay after becoming aware of the data breach.

Failing to notify a breach is in itself a breach.

Controllers and processors should have clear data breach protocols established.

The notification must at least:

- describe the nature of the personal data;
- communicate the name and contact details of the data protection officer or another contact point;
- describe the likely consequences; and

- describe the measures taken to address or mitigate the breach.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

When the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also communicate the breach to the individuals concerned without undue delay.

Specific breach notification requirements apply to providers of publicly available electronic communication services.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

While the law does not set out detailed examples of internal controls to be applied in this regard, under the GDPR, the controllers of PI shall be responsible for, and must be able to demonstrate compliance with, the data protection principles; this should be done through the implementation of appropriate technical and organisational measures, as well as the maintaining of records of processing activities, among other things.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The designation of a data protection officer (DPO) is mandatory only where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations that, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

The DPO is tasked with informing and advising the controller or the processor and the employees on data protection provisions, as well as being responsible to monitor compliance with applicable data protection provisions and with existing policies of the controller or processor concerning the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. The DPO shall also be responsible for providing advice where requested as regards the data protection impact assessment, as well as be responsible for cooperation with the supervisory authority and acting as the contact point for the supervisory authority as well as consulting, where appropriate, concerning any other matter.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

PI owners and processors are obliged to retain written records of the processing activities that they carry out. The records may be retained within the electronic format and are to be made available to the supervisory authority on request.

This obligation of record-keeping shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of individuals, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences. Nevertheless, the enterprise or organisation will still be required to be able to demonstrate its efforts towards compliance, and therefore having some level of internal records will always be advisable.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Regulation (EU) 2016/679 (General Data Protection Regulation) sets out that where new technologies are to be implemented or where the processing operation is likely to result in a high risk, a data protection impact assessment (DPIA) may have to be carried out by the controller. A DPIA shall be required where the processing operation involves a systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. Furthermore, a DPIA shall be required where the processing operation involves many special categories of data, or personal data relating to criminal convictions and offences, as well as when the processing operation involves systematic monitoring of a publicly accessible area on a large scale.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The law obliges controllers to implement measures to apply the privacy-by-design and privacy-by-default principles, and this at the time of the determination of the means for processing and at the time of the processing itself.

The law also sets out that where new technologies are to be implemented or where the processing operation is likely to result in a high risk to the rights and freedoms of natural persons, the controller obliged to, before the processing, carry out a DPIA. The law also provides a non-exhaustive list of particular examples of when a DPIA should be carried out.

Further, before undertaking some types of processing, consultation with the Information and Data Protection Commissioner may be required.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

No.

Other transparency duties

29 | Are there any other public transparency duties?

Regulation (EU) 2016/679 (General Data Protection Regulation) includes principles as well as mandatory requirements requiring controllers to be transparent and clear about the purposes for which they are processing personal data. This obligation is more relevant in respect of the data subjects concerned, rather than an imposition of making public statements at large on the nature of the processing.

The Information and Data Protection Commissioner does require the registration and publication of details appertaining to data protection officers.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The law sets out that controllers shall only engage processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the law.

In addition, the law sets out that the relationship between data controllers and data processors is to be regulated by a written agreement or other legal act that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of PI and categories of data subjects, and the obligations and rights of the controller, among other points.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

If the recipient of PI is a joint controller, then the relationship and sharing of data must be regulated by a joint controllership agreement. In so far as the parties are not joint controllers, or the relationship is not one of a controller-processor relationship, then it would be advisable for the sharing of data to be regulated by a data-sharing agreement.

Restrictions apply to the transfer of PI to third countries or international organisations, in that such transfers must not occur unless certain criteria and conditions are satisfied or exemptions apply.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Transfers to parties established outside of the European Economic Area can only be made where recognised safeguards transfers within EU territory are not prohibited.

A transfer of data can be made to another entity within a third country, where that third country has been declared by the European Commission to offer an adequate level of protection.

If the country to which data is being transferred has not been deemed adequate by the European Commission, then the transfer can be made subject to one of the following data transfer mechanisms:

- binding corporate rules;
- standard contractual clauses;
- approved code of conduct; or
- certification under an approved certification scheme.

Where the transfer is not covered by appropriate safeguards, the transfer can be carried out where it satisfies the criteria of one of the existing derogations set out within article 49 of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR).

The GDPR imposes exclusions of transfers of PI to third countries under foreign court orders or decisions of third-country administrative authorities unless such is expressly provided by EU or Maltese law.

No notification to or authorisation from a supervisory authority is required unless the transfer needs to take place and there is no adequate safeguard or derogation that can be relied upon.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes, the rules on transfers to third countries apply equally to both PI owners and their service providers and onward transfers.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No, there are no localisation rules relating to the processing of PI under local data protection law.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals have the right to obtain from the PI owner confirmation as to whether or not PI concerning him or her is being processed, and a copy of the PI being processed along with detailed information about the processing operation.

The initial response should be free of charge. Where the request is made by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

This right shall not adversely affect the rights and freedoms of others, and therefore the right is not absolute.

If a data subject is not satisfied with the response, a complaint may be lodged with the Information and Data Protection Commissioner. The controller could extend the time to respond if the request is complex or when receiving several requests from the data subject. In such cases, the controller must still reply within one month of receiving their request and explain why the extension is necessary.

If the controller has reasonable doubts concerning the identity of the data subject, it may request the provision of additional information necessary to confirm the identity of the data subject.

Sector-specific legislation may contain limitations on the application of the access right.

Other rights

36 | Do individuals have other substantive rights?

Depending on the processing activity itself, and subject to the application of any exceptions and exemptions, the law recognises the following other substantive rights available to individuals:

- the right to rectification;
- the right to erasure;
- the right to restriction;

- the right to data portability;
- the right to object; and
- the right not to be subject to a decision based solely on automated processing, including profiling.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Any individual who has suffered material or non-material damage as a result of an infringement of the law shall have the right to receive compensation from the controller or processor for the damage suffered. Without prejudice to any other remedy available to him or her, including the right to lodge a complaint with the Supervisory Authority, an individual may, by sworn application filed before the First Hall of the Civil Court, institute an action for an effective judicial remedy against the controller or processor concerned or institute an action for damages against the controller or processor who processes personal data in contravention of the law. Under Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) this includes compensation for moral damages.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

A data subject may have dual recourse. A complaint may be filed with the supervisory authority, which in turn is empowered to enforce the provisions of the GDPR. The data subject may also apply to the courts for damages, without the need of filing a complaint with the authority.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

At the time of writing, controllers and processors may, to a degree, derogate from the provisions regulating the right of access, rectification, restriction and objection for the processing of PI for scientific or historical research purposes or official statistics in particular situations, while in the processing of PI for archiving purposes in the public interest, the controllers and processors may derogate from the provisions regulating all data subject rights where particular criteria have been fulfilled.

Where the PI is processed to exercise the right to freedom of expression and information, including processing for journalistic purposes or the purposes of academic, artistic or literary expression, the controller shall be exempt from complying with a large number of provisions regulating the processing of personal data.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

As a general rule, the storing of information or the gaining of access to information stored in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information by the controller.

These requirements do not prevent the technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network or as may be strictly necessary for the service provider to provide an information society service explicitly requested by the subscriber or user to provide the service.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) addresses direct marketing generally. According to article 21, of the GDPR the data subject always has the right to object to the processing of personal data for direct marketing purposes. If the data subject objects, the controller only has to stop the processing for marketing purposes, but can still process the data for other purposes (eg, for the performance of a contract).

This applies unless special rules with the same regulatory scope are contained in the ePrivacy Directive. Consequently, email marketing is currently only allowed with the consent of the parties concerned. In fact, the Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation No. 586.01), which transposes the ePrivacy Directive, sets out that person shall not use, or cause to be used, any publicly available electronic communications service to make an unsolicited communication for the purpose of direct marketing through an automatic calling machine, a facsimile machine or electronic mail, to a subscriber or user, unless the latter has given his prior consent in writing to the receipt of such a communication.

This is without prejudice to the use of contact details for direct marketing of its own similar products or services, where a person has obtained from his customers their contact details for electronic mail. In this case, however, customers shall be allowed to object, free of charge and easily and simply.

Targeted advertising

42 | Are there any rules on targeted online advertising?

Currently, the law does not set out any specific rules on the undertaking of targeted online advertising, other than if it is based on profiling, the data subject has the right to know about it.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

PI constituting special categories (ie, PI revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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) shall not be processed unless a specific ground provided for in the GDPR is satisfied. Special rules apply to the processing of criminal conviction data and of unique numbers that identify persons.

Profiling

44 | Are there any rules regarding individual profiling?

The law does not set out any specific rules on the use of PI for profiling, other than the obligation on the part of the controller to inform the data subject about the processing in question. The data subject is also granted the right to ask for any decisions to be taken by a human being in lieu of automated decision-making.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There are no express rules or guidance on the use of cloud computing services within the context of data protection and privacy laws. Therefore, the general provisions of the GDPR and the Data Protection Act will apply to the use of cloud computing services.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The years 2020, 2021 and 2022 will be remembered for the global covid-19 pandemic. Public authorities and private organisations had many challenges to deal with, not least that of processing data that appertained to individuals and, for instance, testing for the virus or the inoculation of the vaccine. As with most situations, there is never a one-size-fits-all solution, and it is always the controller who must demonstrate compliance with the law. The covid-19 pandemic also saw an increase in awareness of cybercrime and cybersecurity as the population turned to the online world for the majority of their needs.

The consequences of the *Schrems II* judgment and the possibility of a new Privacy Shield has reignited the discussion on transfers of personal data to third countries. Companies are having to undertake transfer impact assessments, along with the execution of standard contractual clauses, which themselves are in the process of being refreshed.

There are also changes expected to occur to the local landscape further to the transposition of Directive 2018/1972 establishing the European Electronic Communications Code.

FENECH + FENECH
ADVOCATES

Paul Gonzi
paul.gonzi@fenechlaw.com

Sarah Cannataci
sarah.cannataci@fenechlaw.com

198, Old Bakery Street
Valletta, VLT 1455
Malta
Tel +356 2124 1232
www.fenechlaw.com

Mexico

Abraham Diaz, Gustavo A Alcocer and Carla Huitrón
OLIVARES

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The legal framework for PI protection is found in:

- article 6 of the Mexican Constitution:
- the Federal Law for the Protection of Personal Information Held by Private Entities, published in July 2010, and its Regulations published in December 2011;
- the Privacy Notice Rules, published in January 2013;
- the Binding Self-Regulation Parameters, published in January 2013 and May 2014; and
- the General Law for the Protection of Personal Data Held by Public Governmental Entities, published in January 2017.

Mexican PI protection law is not based exclusively on an international instrument on data protection, but instead follows international correlative laws, directives and statutes, and thus has similar principles, regulation scope and provisions.

The Federal Law for the Protection of Personal Data (the Law) regulates the collection, storage, use and transfer of PI and protects individual data subjects' (individuals) rights. It is a federal law of public order that makes its provisions applicable and enforceable at the federal level across the country and is not waivable under any agreement or covenant between parties since it is considered to be a human right. The Law regulates the use and processing given to the PI by PI data controllers (PI controllers) and PI processors, thus providing several rights to individuals and obligations to PI controllers and PI processors, to ensure privacy, security and confidentiality of such information. The Privacy Notice Rules comprise the requirements for such notices, whereas the Binding Self-Regulation Parameters contain the requirements and eligibility parameters to be considered by the authority for approval, supervision and control of self-regulation schemes and authorisation and revocation of certifying entities as approved certifiers. Since June 2018, Mexico has been a member of the Convention for the Protection of Individuals Concerning the Automated Processing of Personal Data, and its Protocol (Convention 108).

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is the data protection authority responsible for overseeing the Law. Its main purpose is the disclosure of government activities, budgets and overall public information, as well as the protection of personal data and individuals' right to privacy. The INAI has the authority to conduct investigations, review and sanction PI controllers and PI processors, and authorise, oversee and revoke certifying entities.

The Ministry of Economy is responsible for informing and educating on the obligations regarding the protection of personal data between national and international corporations with commercial activities in Mexican territory. Among other responsibilities, it must issue the relevant guidelines for the content and scope of the privacy notice in cooperation with the INAI.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Since the Federal Law for the Protection of Personal Information Held by Private Entities proposed a centralised model of protection of PI instead of a sectorial model, the INAI is the only data protection authority in charge of the protection of personal information.

Further, section VII of article 38 of the Federal Law for the Protection of Personal Information Held by Private Entities sets forth as a general obligation of the INAI: 'To cooperate with other supervising authorities and national and international entities, to help in the protection of personal information.'

Likewise, article 40 of the Federal Law for the Protection of Personal Information Held by Private Entities makes clear that this law constitutes the legal framework that any other authorities must observe when issuing any regulations that may imply the processing of PI, and said regulations must be issued in coordination with the INAI. This obligation is also included in articles 77 and 78 of the Regulations of the Federal Law for the Protection of Personal Information Held by Private Entities.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Administrative sanctions are provided for violations to the law from 100 to 320,000 times the minimum general daily wage applicable in Mexico City for PI controllers and PI processors. Depending on the seriousness of the breach and specific behaviour and conduct (profit-making with PI or the methods used to get consent for the use of PI), it may lead to criminal penalties, which are sanctioned with between three months and five years of imprisonment. This also depends on the nature of the PI (penalties are doubled if the personal data is considered by law as sensitive personal data).

Also, related conduct may be sanctioned under the Criminal Code, such as professional secrecy breaches and illegal access to media systems and equipment.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Yes, as this is an administrative procedure, PI owners have two options to appeal an order issued by the data protection authority:

- A remedy claim: this is filed before the same authority that issued the order.
- A nullity trial: this is filed before the Federal Court of Administrative Affairs (FCA), whether appealing the first order issued by the data protection authority or the resolution of the remedy claim. If the resolution issued by the FCA is not satisfactory, it can further be challenged by starting a procedure with the federal circuit courts by the affected party, through an *amparo* lawsuit (a constitutional legal remedy).

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Federal Law for the Protection of Personal Data (the Law) applies to non-public individuals and entities that handle PI. Also, the following non-public persons and entities are excluded from the application of the Law:

- credit information agencies or companies, where such companies are specially regulated by the Law for the Regulation of Credit Information Companies; and
- persons who handle and store PI exclusively for personal use and without any commercial or disclosure purposes.

Also, as from January 2017, the General Law for the Protection of Personal Data Held by Public Governmental Entities applies to any authority, entity, body or organism of the executive, legislative and judicial powers of the government, autonomous entities, political parties, trusts and public funds, at federal, state and municipal levels.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Law covers PI regardless of the means or media where such data is stored, processed or organised (whether physical or electronic); however, there is no regulation regarding the unauthorised interception of communications (as it would relate to surveillance or espionage), electronic marketing or surveillance of individuals. In this regard, such matters as illegal access to media, systems and equipment could be covered by criminal law, including:

- article 166-bis of the Federal Criminal Code sanctions with imprisonment from three months to up to three years, for the person who, in virtue of his or her position in a telecommunications company, unlawfully provides information regarding people using the said telecommunication services;
- article 177 of the Federal Criminal Code sanctions with imprisonment from six to 12 years, and a fine up to 600 the minimum general daily wage (MGDW), for the person who intervenes in any private communication without a judicial order issued by a competent authority;
- article 211-bis of the Federal Criminal Code sanctions with imprisonment from six to 12 years, and a fine up to 600 MGDW, for the person who reveals, divulges or improperly uses any information or images obtained from the intervention of private communication;
- article 36 of the Federal Law for Consumers' Protection sanctions the publication in any mass media of any notice addressed undoubtedly to one or various specific consumers, to collect a debt from them or have them comply with an agreement; and
- article 76-bis of the Federal Law for Consumers' Protection recognises as a consumer's right in transactions effected through electronic, optic or other technologic means, that the supplier of a commodity or service uses the information confidentially provided by the consumer, and consequently said information cannot be transmitted to other different suppliers unless consented by the consumer or ordered by competent authorities.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Along with other laws already pointed out herein, such as the Criminal Code, the Law for the Regulation of Credit Information Companies and the Law for the Protection of Personal Data Held by Public Governmental Entities, there is additional legislation covering specific data protection rules, such as the Civil Code and the Code of Commerce. However, to date, Mexico does not count on specific and express rules for data protection in connection with employee monitoring, e-health records or the use of social media.

In the case of e-health records, there are some specific regulations for the creation and handling thereof. However, concerning the protection of PI, there is a referral to the rules outlined in the Federal Law for the Protection of Personal Information Held by Private Parties, its Regulations, and the General Law for the Protection of Personal Data Held by Public Governmental Entities (the latter in the case of e-health records for the public sector).

Additionally, in January 2021, an amendment to the Federal Labour Law was published and set into force, establishing a general law framework for the regulation of telework. Although this law framework refers to the rules set forth in the Federal Law for the Protection of Personal Information Held by Private Entities, it introduces some rules that must be observed by employers and employees, when operating in telework mode.

PI formats

9 | What categories and types of PI are covered by the law?

The Law covers all types of PI; however, for clarity purposes, the authority divides the PI into the following categories:

- PI:
  - identification data;
  - academic data;
  - transit data and migratory movements;
  - labour data;
  - patrimonial data; and
  - data on administrative and/or judicial procedures; and
- sensitive PI:
  - data on people's health;
  - electronic data;
  - ideological data;
  - biometric data;
  - sexual life data; and
  - ethnic data.

Likewise, the Law covers PI regardless of the means or media used for its storage, process or organisation. Such means or formats include:

- digital formats (eg, hardware, software, web, media, applications, services or any other information-related technology that allows data exchange or processing; among these formats, the Law specifically includes PI stored in the cloud);
- electronic support (ie, storage that can be accessed only by the use of electronic equipment that processes its contents to examine, modify or store the PI, including microfilm); and
- physical support (ie, storage media that does not require any device to process its content to examine, modify or store the PI or any plain sight intelligible storage medium).

Extraterritoriality

10 Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Mexican PI protection laws are not limited to PI controllers established or operating in Mexican territory. Although the Law does not provide a specific reach or scope of its applicability, the Regulations to the Law do. In this regard, such regulations (and, therefore, the Law), in addition to applying to companies established or operating under Mexican law (whether or not located in Mexican territory) apply to companies not established under Mexican law that are subject to Mexican legislation derived from the execution of a contract or under the terms of international law.

Additionally, Mexican regulations on PI protection apply:

- to companies' establishments located in Mexican territory;
- to persons or entities not established in Mexican territory but using means located in such territory, unless such means are used merely for transition purposes that do not imply a processing or handling of PI; and
- when the PI controller is not established in Mexican territory, but the person designated as the party in charge of the control and management of its PI (a service provider) is.

In the case of individuals, the establishment will mean the location of the main place of business or location customarily used to perform their activities or their home.

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

All processing or use of PI is covered by the Mexican legal framework. Mexican PI protection law makes a distinction between PI controllers and those who provide services to controllers, where the latter are independent third parties who may be engaged by the PI controller to be the parties responsible for the PI processing and handling. While it is not mandatory to have this third-party service provider, should a company (PI controller) engage such services, it shall have a written agreement stating clearly all the third party's responsibilities and limitations in connection with the PI.

By virtue of this obligation of PI controllers to execute an agreement with any PI processor they use, the duties acquired by the PI processor must be the same as those imposed by the Law on the PI controller.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The law provides eight main standards for the processing of PI:

- legality: PI controllers must always handle PI according to the law. All personal data shall be lawfully collected and processed, and its collection shall not be made through unlawful or deceitful means;
- consent: PI controllers must obtain consent from individuals for the processing and disclosure of their PI. In this regard, the consent of individuals shall not be required if:
  - PI is contained in publicly available sources;
  - PI cannot be associated with the individual, or if by the way its structure or content cannot be associated with the individual;
  - PI processing is intended to fulfil obligations under a legal relationship between the PI controllers and individuals;
  - an emergency situation exists in which the individual or its properties may be potentially damaged;
  - PI is essential for certain medical or health matters where the individual is unable to provide consent under applicable laws; or
  - a resolution is issued by a competent authority to process and disclose PI, without the required consent;
- information: PI controllers must notify the individual of the existence and main characteristics of the processing that will be given to the PI;
- quality: PI handled must be exact, complete, pertinent, correct and up to date for the purposes for which it has been collected;
- purpose (the finality principle): PI may only be processed to fulfil the purpose or purposes stated in the privacy notice provided to the individual;
- loyalty: PI controllers must protect individuals' interests when handling their PI;
- proportionality: PI controllers may only handle the PI necessary for the purpose of the processing; and
- responsibility: PI controllers are responsible for the processing of the PI under their possession.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

The law makes a distinction regarding 'sensitive' PI. This information is deemed the most personal of the individual, and if mistreated, could lead to discrimination or general risk to the individual (ie, racial or ethnic origin, present or future health status, genetic information, religion, political opinions, trade union membership or sexual orientation).

Given this, the Federal Law for the Protection of Personal Data provides more stringent rules for the processing of this sensitive PI, such as the obligation for PI controllers to always get written and express consent from individuals for the processing of their sensitive PI. Likewise, PI controllers may not hold sensitive PI without justified cause pursuant to the purpose of the processing.

Several additional limitations apply to the general handling of this type of information (eg, PI controllers must use their best efforts to limit the processing term of sensitive PI, the privacy notice must expressly point out the nature of such information when required; and, when it comes to penalties for the breach or mistreatment of PI, these may double when processing sensitive PI).

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The PI controller must have a privacy notice available for all individuals whose data is in their possession or collected for use and processing. According to the Federal Law for the Protection of Personal Data (the Law) and its Regulations, there are three types of privacy notices:

- an integral privacy notice;
- a simplified privacy notice; and
- a short privacy notice.

The privacy notice must include, at least, the following information:

- the identity and address of the PI controller;
- PI that would be subject to processing;
- the purpose of the processing;
- the mechanisms provided by the PI controller to the individuals to limit the use or disclosure of the information;
- the means for individuals to exercise their rights to access, rectify, cancel or oppose the processing of their PI;
- any transfer of the PI to be made, if applicable;
- the procedure and vehicles in which the PI controller will notify individuals about modifications to the privacy notice;
- the procedure and means by which the PI controller should notify the individuals of any modification in such privacy notice; and
- regarding sensitive PI, the privacy notice must expressly state that the information is of a sensitive nature.

In addition, and pursuant to the privacy notice rules, the notice must take into account the following characteristics:

- inaccurate, ambiguous or vague phrases must not be used;
- the individual's profile must be taken into account;
- if an individual's consent is granted through tick marks in text boxes, these must not be pre-ticked; and
- reference to texts or documents not available to individuals must be omitted.

Exemptions from transparency obligations

15 | When is notice not required?

A privacy notice is not necessary when:

- the exemption is available in a specific provision of applicable law;
- the data is available in public sources;
- PI data is subject to a prior dissociation procedure (anonymised data);
- there is an existing legal relationship between the individual and the PI controller;
- there is an emergency situation that could potentially harm an individual or his or her property;
- it is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the individual is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation; or
- a resolution is issued by a competent authority.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Personal information has to fulfil the standard of quality (PI should be exact, complete, pertinent, correct and up to date).

Quality is presumed when PI is provided directly by the individual and remains such until the individual does not express and prove otherwise, or if the PI controller has objective evidence to prove otherwise.

When personal data has not been obtained directly from the individual, the PI controller must take reasonable means to ensure the quality standard is maintained.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Yes, in accordance with the regulation of the Law, only the PI that is necessary, appropriate, relevant and non-excessive in connection with the purposes for which they were obtained may be processed. Therefore, the PI controller must take reasonable efforts to limit the PI processed to the minimum necessary.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The Law provides a 'need-to-hold' basis; PI controllers must not hold PI any longer than the time required to fulfil its purpose (as stated in the privacy notice). After the purpose or purposes have been achieved, any PI controller must delete the data in its collection after blocking them for subsequent suppression.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes, the Law does provide a 'finality principle', whereby a PI controller is restricted to using the PI only to fulfil the purpose or purposes stated in the privacy notice provided to the individuals, the purpose of which must comply with the legality standard. If the PI controller intends to process data for other purposes that are not compatible with, or similar to, the purposes set out in the privacy notice, an individual's consent must be collected again for such additional purposes.

The PI controller is not allowed to use PI for any purposes other than that authorised or notified to the individual, unless such new purpose is authorised by or notified to (in such cases where express authorisation is not required) the individual, or unless such use is explicitly authorised by law or regulation.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

When PI is processed as part of a decision-making process without the intervention of an individual, the PI controller must inform the data subject of this prior to carrying out the process.

Furthermore, as a good practice, the privacy notice may inform the data subject that their PI will be treated as part of an automated decision-making process, explaining the characteristics of the respective process.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

PI controllers or entities in charge of processing PI must take and observe various security measures for the protection of the PI, including administrative, physical and technical measures.

Administrative measures must be taken, such as actions and mechanisms for the management, support and review of the security in the information on an organisational level, the identification and classification of the information, as well as the formation and training of the personnel, in matters of PI.

Also, certain physical measures such as actions and mechanisms – technological or otherwise – are designed to prevent unauthorised access, damage or interference to the physical facilities, organisational critical areas equipment and information, or to protect mobile, portable or easy to remove equipment within or outside the facilities.

Technological measures must also be taken, including controls or mechanisms, with measurable results, that ensure that:

- access to the databases or the information is by authorised personnel only;
- the aforementioned access is only in compliance with authorised personnel's required activities according to his or her duties;
- actions are included to acquire, handle, develop and maintain safety on the systems; and
- there is correct administration on the communications and transactions of the technology resources used for the processing of PI.

Other actions that must be taken include:

- making an inventory of the PI and the systems used for its processing;
- determining the duties and obligations of the people involved in the processing;
- conducting a personal data risk analysis (assessing possible hazards and risks to the PI of the company);
- establishing security measures applicable to PI;
- analysing the identification of security measures already applied and those missing;
- making a work plan for the implementation of any security measures missing as a result of the aforementioned analysis;
- carrying out revisions and audits;
- training to the personnel in charge of the processing of PI; and
- maintaining a register of the PI databases.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

A data breach occurs when data subjects suffer harm or damage to their property or rights because of the PI controller's or processor's non-compliance with any of the provisions stated in the Federal Law for the Protection of Personal Data (the Law).

Under the Law, PI controllers must notify individuals if any of their personal data is breached. Such notice must include:

- the nature of the incident;
- the personal data compromised;
- details on the actions that the individual may adopt to protect his or her interests;
- any corrective actions taking place immediately; and
- any means by which the individuals may find more information on the subject.

In the case of a violation of PI, the PI controllers must analyse the causes of its occurrence and implement the corrective, preventive and improving actions, to adapt the corresponding security measures to avoid the repetition of the violation.

However, to date, Mexican law does not include an obligation for private PI controllers to notify the supervisory authority. Although not required by law, the Mexican data protection authority does, however, recommend the issuing of notices in the event of any data breaches.

Government agencies are obliged to notify the National Institute of Transparency, Access to Information and Personal Data Protection of any data breaches.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Yes, all responsible parties that process PI must establish and maintain physical and technical administrative security measures designed to protect PI from damage, loss, alteration, destruction or unauthorised use, access or processing. They must not adopt security measures inferior to those they keep managing their own information. Moreover, factors such as the risk involved, potential consequences for the data subjects, sensitivity of the data and technological development should be considered.

Administrative security measures

A set of actions and mechanisms should be established to manage, support and review information security at an organisational level, to identify and classify information, and to raise awareness for, educate and train personnel in the protection of PI.

Physical security measures

These include a set of actions and mechanisms, whether they use the technology, intended to protect the PI collected.

Technical security measures

These include a set of activities, controls or mechanisms, which produce measurable results, that use technology to ensure the protection of the PI collected.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There are no criteria stated in the Law that require the appointment of a data protection officer. However, as good practice, the controller should always look to appoint a certified data protection officer who has a certain level of knowledge in PI matters and establish any other desired criteria in the agreement that they will execute.

It is mandatory for the PI controller (or manager) to appoint an officer (person or department) in charge of the PI, who will be in charge of attending to and taking care of individuals' requests to exercise any of their rights provided by the Federal Law for the Protection of Personal

Data (the Law). Likewise, this officer must promote the protection of PI within the company.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Although the Law does not specify record keeping as a mandatory requirement, it is recommended that PI controllers have a PI database, as well as a register on the means and systems used for the storage of those databases to provide the maximum security for the PI under their possession or control. Likewise, it is suggested to keep records as to the consents obtained from individuals for the collecting and processing of their PI.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

No, the Law does not impose owners or processors of PI to carry out a risk assessment in relation to the use of certain PI. However, PI controllers must carry out privacy impact assessments to determine the security measures to be adopted, as outlined in articles 60 and 61 of the Regulations of the Federal Law for the Protection of Personal Information Held by Private Entities.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

No, the Law does not yet include obligations on how PI processing systems must be designed.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no need for PI controllers or processors to register with the National Institute of Transparency, Access to Information and Personal Data Protection (INAI); however, the INAI has the authority to request a surprise inspection to monitor that PI controllers are complying with the Federal Law for the Protection of Personal Data and Regulations.

Registration with the Mexican data protection authorities is neither required by law nor mandatory.

Other transparency duties

29 | Are there any other public transparency duties?

No other public transparency duties are imposed on PI controllers.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

To explain the regulations on transfer of PI, it must first be understood that the Federal Law for the Protection of Personal Data (the Law) defines the transfer of PI as the communication of PI to third parties, whether they are located in Mexico or abroad, other than the PI controller (PI controlling company), in which the third party has to comply with the provisions outlined in the privacy notice of the PI controller.

The transfer of PI to entities that provide PI processing services is not construed as a transfer of PI per se; therefore, any such transfer of PI will be the responsibility of the PI controller and, thus, the PI controller will be liable for any risk or breach in the PI information, which is why it is mandatory to regulate business relationships with PI processors and vendors through the execution of agreements, under which PI processors acquire the same obligations and duties as PI controllers.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Any transfer of PI (as defined by the Law) must be made with the individual's consent unless otherwise provided by the Law (certain exceptions to consent apply). PI disclosure to other recipients must be made under the same conditions as it was received by the PI controller, so, in the case of such disclosure, the PI controller will be able to demonstrate that it was communicated under the conditions as the individual provided such PI. The original PI controller always has the burden of proof in these cases.

As the Law expressly provides that the collecting or processing of any PI has to be through lawful means, the selling or purchasing of PI (marketing lists for advertising purposes), including any PI not collected in accordance with Mexican law, would be deemed illegal. If the marketing list includes only business contact information or publicly available information, then it can be used, and it is always recommended to provide recipients of emails sent for marketing purposes with a mechanism that allows easy opting out from the marketing service.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The following transfers outside the jurisdiction are allowed without restrictions:

- where the transfer is made pursuant to a law or treaty to which Mexico is a party;
- where the transfer is necessary for medical diagnosis or prevention, healthcare delivery, medical treatment or health services management;
- where the transfer is made to holding companies, subsidiaries or affiliates under common control of the PI controller or to a parent company or any company of the same group as the PI controller operating under the same internal processes and policies;
- where the transfer is necessary pursuant to an agreement executed or to be executed in the interest of the individual between the PI controller and a third party;
- where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;
- where the transfer is necessary for the recognition, exercise or defence of rights in a judicial process; and
- where the transfer is necessary to maintain or to comply with a legal relationship between the PI controller and the individual.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Not applicable. Transfers outside the jurisdiction are neither subject to restriction nor authorisation.

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no express provision in Mexican law ordering that a copy of PI be retained in the Mexican jurisdiction when such PI is transferred outside the country; however, the controller who transfers such PI outside the jurisdiction may keep the PI exclusively for the purposes of the responsibilities regarding their treatment.

RIGHTS OF INDIVIDUALS

Access

35 Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Among the main rights of individuals (the right of access, rectification, cancellation and opposition) of the holders on their personal data rights (the rights to access, rectify cancel (request the PI to stop treating their PI) or oppose (ie, refuse) the processing of their PI) is the right to access a copy of the information being held and treated by the PI controller. This right may be limited for national security reasons, regulations on public order, public security and health or for the protection of third-party rights, and with the limitations provided in the applicable laws, or through a resolution of a competent authority.

Other rights

36 Do individuals have other substantive rights?

At any time, the data owner may withdraw his or her consent for the treatment of his or her PI. The controller must establish simple and free mechanisms that allow data subjects to withdraw their consent at least by the same means by which they granted it.

Compensation

37 Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is entitled to declare neither damages nor compensations in favour of any individuals. Therefore, the breach of any PI law does not automatically grant monetary damages or compensation to any PI owner.

Under Mexican legislation, damages must be claimed and proven through a civil law action. Also, injury to feelings can be claimed as moral damage, but moral damages must also be claimed through a civil action before Mexican civil courts. This means that any PI owner has to prosecute first an administrative action before the INAI to prove the breach of the law, and after obtaining a final decision declaring the administrative infringement, it may initiate an independent civil law action, before civil courts to collect any damages, or loses, or to claim any compensation derived from any moral damage.

Enforcement

38 Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights are exercisable by the INAI, which is an administrative agency. The process is initiated either by the filing of an administrative complaint by an affected individual or directly by the INAI, as a result of any anomalies found during a verification procedure.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 Does the law include any derogations, exclusions or limitations other than those already described?

Aside from the limitations and exclusions already described herein, the Federal Law for the Protection of Personal Data does not include any additional derogations, exclusions or limitations.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 Are there any rules on the use of 'cookies' or equivalent technology?

The Federal Law for the Protection of Personal Data (the Law) specifically refers to the use of PI in the cloud; the Law provides a list of requirements any third party providing these types of storage service must comply with to ensure the safety of the PI to be uploaded therein.

Further, when PI controllers use remote or local means of electronic communication, optical or other technology mechanisms, that allow them to collect PI automatically and simultaneously at the same time that individuals have contact with PI (cookies or web beacons), the individuals must be informed, through a communication or warning duly placed in a conspicuous location, concerning the use of these technologies and the fact that PI has been collected, as well as the process to disable such access, except when the technology is required for technical purposes.

Electronic communications marketing

41 Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Law does not provide any specific rules on marketing by email, fax, telephone or other electronic channels; nonetheless, any such contact with individuals is treated as PI and any marketing through those media will, therefore, be regulated according to the Law.

Targeted advertising

42 Are there any rules on targeted online advertising?

All advertising that is directed to consumers in Mexico is governed by the Federal Consumer Protection Law;, there are no specific regulations for targeted online advertising (online behavioural advertising), but the Federal Bureau for Consumer Protection operates a call-blocking registry, covering landlines and mobile phone numbers, which gives suppliers making advertising calls and sending advertising messages 30 days to stop disturbing the consumer at his or her registered address or electronic address or by any other means.

Likewise, all the advertising purposes must be specified clearly in the privacy notice, and the owner's consent is required.

Sensitive personal information

43 Are there any rules on the processing of 'sensitive' categories of personal information?

The Law describes as sensitive PI any PI that may affect the most intimate sphere of an individual, or that which, if misused, may lead to discrimination or carry a serious risk to the individual. In particular,

sensitive personal information is considered that which may reveal information such as ethnic or racial origin, a present or future medical condition, genetic information, religious, philosophical and moral beliefs, union affiliation, political opinions and sexual preference.

Express and written consent is required from the PI's owner for its treatment. No database with sensitive PI may be created without a legitimate justification, and they must be created in accordance with the explicit purposes of the controller.

Databases containing sensitive PI may only be created if:

- they obey to a legal mandate;
- it is justified for national security matters, public order, public security and public health, as well as to protect the rights of third parties; or
- the controller requires it for legitimate, concrete purposes and in accordance with his or her explicit purposes.

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific rules on individual profiling; however, if such automated processing results in personal data or information that may identify an individual, such activity will be subject to the Law, in which case the controller will be responsible under the Law.

Further, such advertising purpose will have to be clearly specified in the privacy notice, and the owner's consent will be required.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Mexican law regulates the processing of PI in services, applications, and infrastructure in cloud computing. That is the external provision of computer services on demand that involves the supply of infrastructure, platform, or software distributed flexibly, using virtual procedures, on resources dynamically shared. For these purposes, the data controller may resort to cloud computing by general contractual conditions or clauses.

These services may only be used when the provider complies at least with the following:

- has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;
- makes transparent subcontracting that involves information about the service that is provided;
- abstains from including conditions in providing the service that authorises or permits it to assume the ownership of the information about which the service is provided;
- maintains confidentiality concerning the personal data for which it provides the service; and
- has mechanisms at least for:
    - disclosing changes in its privacy policies or conditions of the service it provides;
    - permitting the data controller to limit the type of processing of personal data for which it provides the service;
    - establishing and maintaining adequate security measures to protect the personal data for which it provides the service;
    - ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it; and
    - impeding access to personal data by those who do not have proper authorisation for access or in the event of a request duly made by a competent authority and informing data controller.

In any case, the data controller may not use services that do not ensure the proper protection of PI.

No guidelines have yet been issued to regulate the processing of PI in cloud computing.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

On 16 April 2021, an amendment to the Federal Telecommunications and Broadcasting Law was published in the Official Gazette, aimed at the creation of a national registry of mobile phone users, through which it is intended to create a database with information on individuals or legal entities who own mobile phones.

The registration of mobile phone numbers, including all of the aforementioned requirements, was mandatory for all users of mobile phones in Mexico, and the telecommunications concessionaires would be responsible for collecting and updating or modifying the users' information, which will be available for Mexican competent authorities.

This reform caused alarm among specialists in the field, as well as among users in general, due to the lack of security observed in the past in the handling of personal data by the government, as well as the disproportionate demands it places on mobile phone users, forcing them to reveal sensitive data such as biometric data, in contravention to international trends.

The Mexican data protection authority (the National Institute of Transparency, Access to Information and Personal Data Protection (INAI)) filed a legal action denouncing the unconstitutionality and illegality of this amendment and, in May 2022, the Mexican Supreme Court of Justice ruled that the action filed by INAI was legally grounded, thus declaring as illegal the creation of the above-mentioned registry. This decision is final.

OLIVARES
we know

Abraham Díaz
abraham.diaz@olivares.mx

Gustavo A Alcocer
gustavo.alcocer@olivares.mx

Carla Huitrón
Carla.huitron@olivares.mx

Pedro Luis Ogazón 17
San Angel
01000
Mexico City
Mexico
Tel: +52 55 5322 3000
Fax: +52 55 5322 3001
www.olivares.com.mx

As to initiatives aimed at the proper management of PI during the covid-19 pandemic, there was no emergency legislation in Mexico, and the relief programmes observed in the Mexican government were focused on enhancing the awareness of the value of PI among PI owners, so that they were more careful when sharing their PI, amidst a very relevant booming in the use of e-commerce platforms. INAI was very active in spreading official communications teaching PI owners as to how to safeguard one's PI. Likewise, INAI was heavily focused on enhancing its technological tools so that PI owners could exercise its rights though electronic means and data controllers and data processors could receive any legal assessment and consultation from INAI through such electronic means.

Finally, INAI was very active in keeping surveillance on the proper collecting and processing of PI by data controllers and data processors, and initiated a relevant number of proceedings and imposed a significant number of relevant sanctions against private and public entities who were found in default of the obligations set forth in Mexican law.

New Zealand

Derek Roth-Biester, Megan Pearce and Emily Peart

Anderson Lloyd

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The protection of PI is primarily governed by the Privacy Act 2020 (the Act). The Act regulates the collection, storage, security, access and correction and other dealings with PI by both public- and private-sector organisations (referred to in the Act as 'agencies'). The Act adopts a principle-based framework centralised around 13 information privacy principles (IPPs). These IPPs originate from the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which was adopted in 1980.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Privacy Commissioner (the Commissioner) appointed under the Act is responsible for monitoring the operation of the Act in New Zealand as well as examining any proposed legislation or policy that the Commissioner considers may affect the privacy of individuals.

The Commissioner can instigate an investigation into an agency's dealings with PI on the Commissioner's initiative. The Commissioner may also (but is not always obliged to) instigate an investigation of an agency's dealings with PI as a result of a submitted complaint.

When investigating an agency's dealings with PI, the Commissioner can largely regulate their own procedure as they see fit (subject to the Act and its regulations).

When requested to do so by any agency, the Commissioner can conduct an audit of PI maintained by that agency to ascertain whether the information is maintained according to the IPPs.

The Commissioner can issue compliance notices requiring agencies to either do or stop doing something should the Commissioner consider that the agency has breached the Act or any code of practice issued under the Act. The penalty for failing to comply with a compliance notice can be up to NZ$10,000.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There is no express legal obligation under the Act for the Commissioner to cooperate with international data protection authorities. New Zealand is not currently a party to any binding cross-border privacy schemes, such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System.

Under the Act, the Commissioner may refer matters to an overseas privacy enforcement authority where the complaint relates to a matter that is more properly within its jurisdiction.

The Commissioner, as a matter of good practice, continues to engage with the premier global network of privacy commissioners as a founding member of the Global Privacy Enforcement Network and a participant in the APEC Cooperation Arrangement for Cross-Border Privacy Enforcement. The Commissioner of New Zealand and Australia signed a memorandum of understanding (MOU) in 2008 to facilitate cooperation between their offices on privacy-related issues (including information sharing). However, the MOU is not intended to be legally binding but rather to provide a practical means of meeting the cooperation targets set out in the APEC Privacy Framework.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under the Act, the Human Rights Review Tribunal (the Tribunal) can award damages for interference with an individual's privacy.

The Commissioner has the authority to make binding decisions on complaints about information access requests, not the Tribunal (although such decisions will be subject to a right of appeal to the Tribunal).

Following an investigation of any privacy complaint by the Commissioner, proceedings can be brought in the Tribunal in respect of the complaint in certain circumstances (including where the Commissioner has decided not to investigate the complaint). The Tribunal may award damages in respect of the interference with the privacy of an individual as compensation for the humiliation, loss of dignity and injury to feelings caused by serious breaches, as well as the loss of any benefit (monetary or other) that the individual might reasonably have expected to obtain if the interference had not occurred.

Under the Act, a person may be liable on conviction to a fine not exceeding NZ$10,000 for certain breaches of the Act including: (1) misleading an entity to obtain access to someone else's personal information and (2) destroying a document containing personal information with knowledge of a request related to it. Furthermore, under

the Crimes Act 1961, criminal penalties are available in respect of the unlawful interception of private communications, as well as certain unlawful monitoring and surveillance activities.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

If an agency disagrees with an access direction made by the Commissioner, an agency can appeal to the Tribunal against the direction. The agency has 20 working days from receiving the notice to lodge its appeal unless exceptional circumstances apply. The Commissioner has a right to be heard in any appeal.

The Tribunal may determine an appeal by confirming the direction appealed against, modifying the direction or reversing the direction order.

If the agency then fails to follow the Tribunal's orders or directions, the decision can be enforced in the District Court.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Privacy Act 2020 (the Act) generally applies to:

- New Zealand residents and businesses;
- overseas businesses in the course of carrying on business in New Zealand; and
- individuals not resident in New Zealand in relation to PI collected or held while in New Zealand.

New Zealand data protection law generally covers all sectors and organisations; however, certain agencies are excluded from application of the Act including:

- members of Parliament;
- courts and tribunals in relation to their judicial functions; and
- the news media when it relates to the collection and reporting of news and current affairs.

While New Zealand's intelligence and security agencies are not excluded wholesale from the application of the Act, non-compliance with certain information privacy principles (IPPs) is permitted under the Act to the extent the non-compliance is necessary to enable an intelligence and security agency to perform any of its functions.

Additionally, individuals who collect or hold PI for their own personal, family or household affairs are exempt from the IPPs (although this does not apply where the collection, disclosure or use would be highly offensive to an ordinary reasonable person).

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Act does not expressly cover interception of communications, electronic marketing or monitoring and surveillance of individuals; although, the IPPs will apply in respect of the collection and processing of any PI collected through monitoring and surveillance activities. The relevant law in this regard is as follows:

- Under the Crimes Act 1961 (Crimes Act), a person faces up to two years' imprisonment if they intentionally intercept any private communications through an interception device (eg, recording device), other than when they are authorised to do so under other legislation (eg, the Search and Surveillance Act 2012). Any intentional disclosure of private communication, the substance and meaning of that communication or intentional disclosure of the existence of private communication could result in up to two years' imprisonment.
- Further, under the Crimes Act, there are criminal penalties for restricted monitoring and surveillance activities, including intimate visual recordings. Any individual that intentionally or recklessly makes, possesses (in certain circumstances) and publishes, imports or sells intimate visual recordings of another person is liable to imprisonment.
- The Search and Surveillance Act 2012 regulates police powers and their ability to monitor compliance with the law and their power to carry out investigations and the prosecution of offences.
- The Unsolicited Electronic Messages Act (2007) governs the sending of commercial electronic messages and prohibits the sending of unsolicited commercial electronic messages, in particular the use of address-harvesting software. It applies to any electronic message sent for a commercial purpose. 'Electronic message' is defined broadly to cover any form of message sent using a telecommunications service (but excluding voice calls) or to an electronic address, and therefore covers email, fax, text messages and other forms of electronic messages.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

The Privacy Commissioner (the Commissioner) may, from time to time, issue codes of practices under the Act to supplement the IPPs in respect of certain classes of information or certain classes of agency.

There are currently six codes of practice in operation: the Civil Defence National Emergencies (Information Sharing) Code, the Credit Reporting Privacy Code, the Health Information Privacy Code, the Justice Sector Unique Identifier Code, the Superannuation Schemes Unique Identifier Code and the Telecommunications Information Privacy Code.

PI formats

9 | What categories and types of PI are covered by the law?

All categories and types of PI are covered by the Act. Any information that falls within the definition of PI under the Act (ie, information about an identifiable individual) is protected.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Act applies to overseas agencies to the extent they are carrying on business in New Zealand, regardless of where the agency is physically based or operating from.

The Act aligns its application to extraterritorial agencies with the position under the EU General Data Protection Regulation (GDPR). Some overseas entities may be deemed agencies carrying on business in New Zealand regardless of whether or not they:

- do so as a commercial operation or with an intent to make a profit;
- have a physical presence in New Zealand; or
- receive any payment for the supply of goods or services.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The Act covers all uses of PI by an agency (with specific codes of practice modifying the Act for particular sectors).

The Act does not expressly distinguish between data controllers and data owners; however, the Act provides that where an agent (A) holds PI as an agent for another agency (B) (eg, for safe custody or processing), then PI is treated as being held by B and not A (unless A also uses or discloses the PI for its own purposes). Agencies that provide processing services to the original owner of the PI as its agent (ie, cloud providers and other service providers that process information on behalf of others) will still be held accountable for the PI that they hold, store and process to the extent that they use or disclose the information for their own purposes.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Under the Privacy Act 2020 (the Act), PI must not be collected unless the collection is for a lawful purpose connected with a function or activity of the agency and the collection is necessary for that purpose. If the lawful purpose for which the agency intends to collect PI does not require the collection of an individual's information, then that agency may not require the individual's information.

There are also limits on how PI can be used once it has been collected. PI that was obtained in connection with one purpose cannot be used for any other purpose unless:

- consent is obtained;
- the information is already in the public domain; or
- non-compliance is required in the circumstances (ie, to enforce the law, to protect public revenue, for the conduct of proceedings before a court or tribunal or to prevent or lessen a serious threat).

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

The Act does not expressly impose more stringent rules for processing specific categories and types of PI; however, codes of practice issued under the Act may modify the application of the information privacy principles under the Act to specific categories and types of PI. For example, codes of practice specifically regulating PI held for credit reporting purposes, health information and telecoms information have been issued in New Zealand.

The criminal records of those who are deemed to have a clean criminal record (subject to specific protection under the Clean Records (Clean Slate) Act 2004) may be processed only for purposes allowed by that Act.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The Privacy Act 2020 (the Act) requires agencies collecting PI directly from an individual to take steps that are reasonable in the circumstances to ensure that the individual is aware of certain information, including:

- the fact that the information is being collected;
- the purpose for which the information is being collected;
- the intended recipients of the information;
- the consequences for them if they do not provide all or part of the requested information; and
- how they may request access to and correction of PI.

Where the collection of PI is authorised or required by law, the individual must be also informed of the particular law by which the collection of the information is authorised or required, as well as whether the supply of the information is voluntary or mandatory.

Exemptions from transparency obligations

15 | When is notice not required?

Notice is not required where either the collecting agency has taken the necessary steps concerning the collection of the same or similar information from the individual on a recent previous occasion or if the agency believes, on reasonable grounds, that:

- non-compliance would not prejudice the interests of the individual concerned;
- the non-compliance is necessary to avoid prejudice to the maintenance or enforcement of the law (including the conduct of proceedings before any court or tribunal);
- the non-compliance is necessary for the protection of public revenue;
- compliance is not reasonably practicable in the circumstances of the particular case; or
- where the PI collected will not be used in a form in which the individual concerned can be identified.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes. Under the Act, no agency may use or disclose PI without taking reasonable steps to ensure that, having regard to the purpose for which the PI is proposed to be used, the PI is accurate, up to date, complete, relevant and not misleading.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

While there are no express restrictions on the types or volume of PI collected, information privacy principles require that PI must not be collected by an agency unless it is collected for lawful purposes connected with the function or activity of the agency and the collection is necessary for that purpose.

Data retention

18 Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

While there are no prescribed time frames for retention of PI under the Act, agencies must not keep PI for any longer than is required for the purposes for which the PI may lawfully be used.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes. As a general principle, any agency that holds PI must use that PI only for the purposes in respect of which the PI was obtained.

Under the Act, an agency holding PI may use that PI for a purpose other than the purposes in respect of which that PI was originally obtained where the agency reasonably believes:

- that the individual concerned has authorised the new use;
- that the source of the information is publicly available and it would not be unfair or unreasonable to use the information;
- the non-compliance is necessary to avoid prejudice to the maintenance or enforcement of law (including the conduct of proceedings before any court or tribunal);
- the non-compliance is necessary to prevent or lessen a serious public threat or the safety of the individual concerned;
- the PI will not be used in a form in which the individual concerned can be identified;
- the use is necessary to enable a New Zealand intelligence or security agency to perform its functions; or
- the disclosure is necessary to facilitate the sale of a business as a going concern.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The Act does not expressly cover automated decision-making; however, agencies must have regard to the original purpose of collection when using that PI for profiling.

The Privacy Commissioner, in carrying out automated decision-making, recommended that the government's use of algorithms retains an element of human oversight on the grounds that analytical processes should never entirely replace human oversight. However, it has been acknowledged that as technology continues to evolve, the government will need to keep an eye on the balance between the importance of human oversight and possible efficiencies and improvements in service delivery.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Privacy Act 2020 (the Act) requires that agencies protect PI with such security safeguards as it is reasonable in the circumstances to take against loss, access, use, modification, disclosure and other misuse.

If it is necessary for the PI to be processed by a third-party service provider, the agency must do everything reasonably within its power to prevent unauthorised use or unauthorised disclosure of the PI by that service provider.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The Act sets out a process for the management of a 'notifiable privacy breach' – that is, a privacy breach that causes, or is likely to cause, serious harm to an affected individual.

The Act mandates that agencies must notify the Privacy Commissioner as soon as is practicable after becoming aware that a notifiable privacy breach has occurred. An agency is also required to notify affected individuals as soon as practicable after becoming aware that a notifiable privacy breach has occurred, unless it is not reasonably practicable, in which case a public notice is required unless an exception or delay applies.

While not an express requirement of the Act, the commissioner has provided that, as a guide, it is expected that a breach notification should be made to the Office of the Privacy Commissioner no later than 72 hours after the agency is made aware of the breach.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

There is no express requirement for agencies to implement self-auditing internal controls. However, under the Privacy Act 2020 (the Act) agencies must ensure that there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of PI.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The Act requires agencies to have at least one privacy officer (either from within or outside the agency).

The legal responsibilities of the data protection officer are, namely: encouraging the agency to comply with the information privacy principles (IPPs); dealing with requests made to the agency under the Act (eg, access requests); working with the Office of the Privacy Commissioner (OPC) in relation to investigations conducted pursuant to complaints made under the Act in relation to the agency; and otherwise ensuring compliance by the agency with the Act.

While there is no specific criteria for who qualifies for appointment as a privacy officer, the OPC recommends that the privacy officer should be familiar with the Act, IPPs and any other relevant regulations. Furthermore, they should be able to deal with complaints from individuals of alleged interferences with PI and train staff in agencies on best privacy management practices.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The Act does not expressly require agencies holding or processing PI to maintain specific internal records or establish internal processes. The Act imposes a high-level obligation on agencies to:

- only hold PI for as long as is required for the purpose it may lawfully be used for;
- ensure that any PI held by that agency is protected; and
- take reasonable security safeguards to protect the PI against:
  - loss;
  - access;
  - use;
  - modification;
  - disclosure; or
  - another misuse.

The IPPs naturally drive agencies to develop such internal processes.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

There are no express requirements to carry out risk assessments under the Act. However, a privacy impact assessment (PIA) is a tool voluntarily utilised by agencies to identify the potential risks arising from their collection, use or handling of PI under the Act and help ensure compliance with the IPPs. The privacy commissioner views a PIA as an increasingly useful tool that agencies of all sizes can fit within their existing internal policies to help them manage privacy more successfully.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The Act contains no specific legal obligations on new processing operations to, for example, integrate data protection measures into an agency's processing activities and operations at the design stage.

To comply with many of the IPPs set out in the Act (including the restrictions on using and disclosing any PI other than for the purpose in connection with which the PI was obtained), most new PI processing operations will integrate data protection measures to ensure compliance with the Act into their business practices from launch and throughout the operation's lifecycle.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

No.

Other transparency duties

29 | Are there any other public transparency duties?

No.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Privacy Act 2020 (the Act) does not specifically regulate the transfer of PI with third-party processors. However, where an agency (1) holds PI as an agent for, or for the sole purpose of processing the information on behalf of, another agency and (2) does not use or disclose the PI for its own purposes, the Act treats this as information held by the agency on whose behalf it is held or processed. Furthermore, the agency will then be liable for the acts or omissions of its agent regarding the processing of PI, unless done or omitted without the agency's express or implied authority. The commissioner has produced an array of simple contractual clauses that agencies can adopt to help ensure that PI will be subject to appropriate contractual controls.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Under the Act there is a general restriction against disclosure for any purpose that is not one of the purposes in connection with which the information was obtained.

An agency must not disclose PI to any other agency unless it believes on reasonable grounds:

- that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained;
- that the disclosure is to the individual concerned;
- that the disclosure is authorised by the individual concerned;
- that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information;
- that the disclosure of the information is necessary:
  - to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution and punishment of offences;
  - for the enforcement of a law that imposes a pecuniary penalty;
  - for the protection of public revenue; or
  - for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);
- that the disclosure of the information is necessary to prevent or lessen a serious threat to:
  - public health or public safety; or
  - the life or health of the individual concerned or another individual;
- that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions;
- that the information:
  - is to be used in a form in which the individual concerned is not identified; or
  - is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Under the Act, agencies are only able to disclose PI to foreign persons or entities if:

- the individual authorised the disclosure (after having been expressly informed by the agency that the overseas person may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the Act);

- the overseas person is otherwise 'carrying on business in New Zealand', such that the agency reasonably believes that the overseas person is subject to the Act;
- the overseas person is subject to the laws of a 'prescribed country' or a participant in a 'prescribed scheme'. Noting that as of May 2022 there are no prescribed countries or prescribed schemes that have been approved as such by regulations to the Act; or
- the agency believes on reasonable grounds that the overseas person is required to protect the PI in a manner comparable to that required by the agency under New Zealand law.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restriction against the disclosure of PI to overseas persons under the Act will usually not apply to transfers to cloud storage providers or other overseas processors (to the extent that entity is engaged on behalf of another agent under a services or agency arrangement and is not otherwise using the PI for its own purposes). Responsibility of the storage and security of PI will remain with the PI owner.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes. The individual to whom the particular PI relates has a right to receive, upon request, confirmation from the agency of whether or not it holds such PI and a right to access the PI.

If an agency receives a request for access to an individual's PI, it has 20 working days to respond to the request (including stipulating what charge may be applied in respect of the management of the request). This time limit may be extended if the request is for a large quantity of information or consultation with other third parties is required in respect of the request.

The Privacy Commissioner (the Commissioner) will make binding decisions on complaints about information access requests, rather than the Human Rights Review Tribunal (the Tribunal); although, such decisions are subject to a right of appeal to the Tribunal.

Other rights

36 | Do individuals have other substantive rights?

Where an agency holds PI about an individual, that individual can request the correction of their PI.

Where an agency that holds PI is not willing to correct that information following a request by the individual concerned, the agency will, if so requested by the individual, take reasonable steps to attach a statement that a correction of the relevant PI has been sought.

In New Zealand, there is currently no express right that entitles individuals to request that an agency delete their PI.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Following an investigation of any privacy complaint by the Commissioner, if the alleged interference cannot be settled between the relevant parties, proceedings can be brought in the Tribunal and remedies sought can include damages. The tribunal may award damages in respect of the interference with the privacy of an individual to appropriately compensate them for the humiliation, loss of dignity and injury to feelings caused by serious breaches, as well as the loss of any benefit (monetary or other) that the individual might reasonably have expected to obtain if the interference had not occurred.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The enforcement of the Privacy Act 2020 (the Act) (including an agency's compliance with any access request) is primarily the responsibility of the Commissioner or the authorities to which the Commissioner delegates its investigations. If following the relevant investigation by the Commissioner the complaint cannot be settled between the relevant parties, proceedings can be brought in the Tribunal. If the aggrieved individual disagrees with the Tribunal's decision, it can be appealed to the High Court. In which case, the judiciary can play a role in enforcing the Act.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Information privacy principles are not intended to apply to the collection of PI by an agency that is an individual where that PI is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family or household affairs. However, this exclusion will not apply once the relevant PI is collected, disclosed or used, if such collection, disclosure or use would reasonably be considered highly offensive.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Currently, the Privacy Act 2020 (the Act) does not contain any express provisions regarding cookies or equivalent technology. Information privacy principles (IPPs) will apply in respect of PI collected via cookies or similar technologies.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

The Unsolicited Electronic Messages Act 2007 (UEMA) regulates the conditions for direct marketing by email, instant messages, texts and fax. The UEMA requires that all commercial electronic messages: may only be sent with the consent of the recipient; must include accurate information about the individual who authorised the sending of the

message; and must include a functional unsubscribe facility. Certain commercial emails (ie, messages that provide factual information about the goods acquired, a subscription, a membership, an account, a loan or a similar ongoing relationship) are not be deemed commercial electronic messages and, therefore, will not be subject to the restrictions under the UEMA.

There is no specific legislative scheme limiting direct marketing by telephone to individual subscribers, and voice calls made using a standard telephone service are specifically excluded from the scope of the UEMA. However, telemarketing activities that collect and store personal data must comply with the Act, IPPs and other enactments.

Targeted advertising

42 | Are there any rules on targeted online advertising?

Currently, the Act does not contain any express provisions regarding targeted online advertising or behavioural advertising. The IPPs will apply in respect of PI used for such advertising.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

There are no specific restrictions relevant to the processing of 'sensitive' categories of PI under the Act.

However, if PI is sensitive, this may influence the application of certain processes under the Act. For example, in assessing whether a privacy breach has caused 'serious harm', the nature of the PI (whether sensitive or not) will be considered among other factors.

Profiling

44 | Are there any rules regarding individual profiling?

There are no express requirements or regulations related to the various uses of data profiling. However, the IPPs will apply to agencies use of PI for individual profiling.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Cloud computing services are not specifically regulated under the Act. The privacy commissioner released a guide titled 'Cloud Computing: A guide to making the right choices' in February 2013 outlining some high-level guidance for businesses looking to move into cloud computing. This guidance includes a 10-step checklist for small businesses that asks small businesses to, among other things:

- ensure adequate research is carried out on the relevant provider;
- understand what business information and personally identifiable information will be stored by the provider; and
- understand how the provider will see the business' information and how the information can be accessed, managed and deleted as necessary once it has been stored on the cloud.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The global pandemic has seen a significant shift in the way PI is handled. We are now required to share more PI online, rather than simply choosing to exercise an option to share PI online, to operate in society.

anderson lloyd.

Derek Roth-Biester
derek.roth-biester@al.nz

Megan Pearce
megan.pearce@al.nz

Emily Peart
emily.peart@al.nz

Level 3
Australis Nathan Building
37 Galway Street
Britomart
Auckland 1010
New Zealand
Tel: +64 9 338 8300
www.al.nz

According to the Privacy Commissioner, the emergence of covid-19 has accelerated the trend of us living more online. Therefore, while there is a sense of acceptance and inevitability in sharing PI, there is an increasing responsibility that lies with the agents and agencies to ensure they are, in turn, looking after that PI. The future will see more rigorous privacy policies being implemented, more efficient cyber-incident response procedures and continual assessment and introduction of amendments and regulations to fit the current privacy landscape.

Likewise, increasing use of biometric technology during the pandemic has led to calls for greater regulation of biometrics. While it is the Office of the Privacy Commissioner's view that the information privacy principles and the regulatory tools in the Privacy Act 2020 are currently sufficient to regulate the use of biometrics from a privacy perspective, it will be a case of frequent re-evaluation whether significant privacy issues or regulatory gaps have emerged.

Pakistan

Saifullah Khan and Saeed Hasan Khan

S.U.Khan Associates Corporate & Legal Consultants

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Pakistan is in the process of developing a dedicated law on personal data protection. The Ministry of Information Technology and Telecommunication has developed a draft of the law, the Personal Data Protection Bill 2021 (the draft Bill). The draft Bill has passed the consultation stage, and the Federal Cabinet has also approved it. The draft Bill will now be tabled before the legislature, the National Assembly and the Senate, for promulgating the law. PI is called 'personal data' in the draft Bill to mean any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data, provided that anonymised, encrypted or pseudonymised data that is incapable of identifying an individual is not personal data. The answers to the following questions are based upon the draft Bill. The draft Bill largely follows the General Data Protection Regulation of the European Union.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The federal government, under the draft Bill, is to establish a commission to be known as the National Commission for Personal Data Protection of Pakistan (the Commission). On promulgation of the law (the draft Bill becoming an Act), the federal government will establish the Commission. The Commission, under the draft Bill, shall be responsible to carry out the purposes of the draft Bill. The Commission shall be competent to decide complaints and pass any order. To decide complaints the Commission shall be deemed to be Civil Court and shall have the same powers as are vested in the Civil Court. The Commission shall be empowered to formulate a compliance framework concerning data audits. The Commission may require a data controller or a data processor to provide such information to the Commission as may reasonably be required for effective discharging of functions of the Commission.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The draft Bill provides that the Commission may, subject to prior approval of the federal government, cooperate with any foreign authority or international organisation in the field of data protection, data security, data theft or unlawful data transfer. The cooperation is to be based on the terms and conditions of any programme or agreement for cooperation to which such foreign authority or international organisation is a party or pursuant to any other international agreement made after the commencement of the draft Bill.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The draft Bill provides for the following penalties concerning contravention of the provisions of the draft Bill:

Offence	Fine/imprisonment
A data controller not ceasing the processing of personal data after withdrawal of consent by the data subject	A fine of up to 5 million Pakistani rupees
Anyone who processes or causes to be processed, disseminates or discloses personal data in violation of the draft Bill	A fine of up to 15 million Pakistani rupees and in the case of subsequent unlawful processing the fine may be raised to 25 million Pakistani rupees. In the case of sensitive data, the fine may be raised to 25 million Pakistani rupees
Failure to adopt the security measures that are necessary to ensure data security	A fine of up to 5 million Pakistani rupees
Failure to comply with the orders of the Commission or the direction of the Commission	A fine of up to 2.5 million Pakistani rupees, or a fine of up to 250 million Pakistani rupees or suspension or termination of the registration and the imposition of additional conditions
Corporate liability on a legal person	A fine not exceeding 1 per cent of its annual gross revenue in Pakistan or 30 million Pakistani rupees, whichever is greater

The Commission will be empowered to formulate a compliance framework concerning personal data breach and grievance redressal mechanism. Once this compliance framework is formulated then it will be clear as to how to deal with such breaches.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Any decision of the Commission is appealable before the High Court or to any tribunal established by the federal government in the manner prescribed by the High Court.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data Protection Bill 2021 (the draft Bill) applies to all sectors and types of organisations. However, it provides an exemption to specific processing from a few specified requirements, as follows:

- the prevention or detection of crime or for investigations;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax or duty or any other imposition of a similar nature;
- preparing statistics or carrying out research (provided that resulting statistics or results of the research are not made available in a form that identifies the data subject);
- the connection with any order or judgment of a court;
- the discharging of regulatory functions (if the application whereof would be likely to prejudice the proper discharge of those functions); and
- journalistic, literary or artistic (subject to certain conditions).

The above-stated are exempted from the following requirements:

- the general requirements (of lawful purpose, purpose limitation, data minimisation and consent);
- notice to the data subject;
- non-disclosure; and
- adherence to the security standards prescribed by the National Commission for Personal Data Protection of Pakistan (the Commission).

Also, the processing concerning the physical or mental health of data subject is exempted from the applicability of security standards prescribed by the Commission if application whereof would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

The draft Bill is not applicable for personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The draft Bill does not cover interception of communication and surveillance of individuals.

The Investigation for Fair Trial Act 2013 provides for investigation for collection of evidence through modern techniques and devices to prevent and effectively deal with certain specified offences.

The Monitoring and Reconciliation of Telephony Traffic Regulations 2010 deals with controlling grey traffic. These Regulations are applicable for licences issued by the Pakistan Telecommunication Authority for:

- long-distance and international;
- infrastructure or landing station;
- local loop (fixed and wireless); and
- cellular mobile.

As regards electronic marketing or monitoring, the draft Bill provides a right for the data subject not to be subjected to a decision solely based on automated processing including profiling.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

- Banking:
  - the Payment Systems and Electronic Fund Transfers Act 2007;
  - the State Bank of Pakistan (SBP) Regulations for Payment Card Security; and
  - the SBP Regulations for Security of Internet Banking; and
- telecommunications:
  - the Telecom Consumer Protection Regulations 2009;
  - the Regulations for Technical Implementation of Mobile Banking 2016; and
  - the Critical Telecom Data and Infrastructure Security Regulations 2020.

PI formats

9 | What categories and types of PI are covered by the law?

The draft Bill covers personal data in an all-inclusive way (any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data, provided that anonymised, encrypted or pseudonymised data that is incapable of identifying an individual is not personal data). The draft Bill covers all processing of personal data whether or not by automated means.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The draft Bill has extraterritorial applicability. The draft Bill is applicable to a data controller or data processor who is digitally or non-digitally operational in Pakistan but is incorporated outside Pakistan and is involved in commercial or non-commercial activity in Pakistan. The draft Bill is also applicable to the processing of personal data by a data controller or data processor not established in Pakistan but in a place where the law of Pakistan applies owing to private and public international law.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The draft Bill applies to the processing of personal data either by a data controller or by a data processor.

'Data controller' means a natural or legal person or the government, who either alone or jointly has the authority to decide on the collection, obtaining, usage or disclosure of personal data.

'Data processor' means a natural or legal person or the government who alone or in conjunction with others processes data on behalf of the data controller.

The draft Bill places significant obligations on the data controllers and there are lessor obligations on the data processors as compared to data controllers. The data processors, however, are responsible for ensuring compliance with security standards prescribed by the Commission. The Commission is empowered to formulate a compliance framework for data processors. A complaint can also be filed against both the data controllers and data processors.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Section 5 of the Personal Data Protection Bill 2021 (the draft Bill) lays down the general requirements for personal data collection and processing. Personal data shall not be processed unless:

- the personal data is processed for a lawful purpose directly related to an activity of the data controller;
- the processing of the personal data is necessary for, or directly related to, that purpose; and
- the personal data is adequate but not excessive concerning that purpose.

A data controller, under the draft Bill, shall not process personal data unless the data subject has given his or her consent. Following are the exceptions to have consent:

- for the performance of a contract to which the data subject is a party;
- for taking steps at the request of the data subject to enter into a contract;
- for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;
- to protect the vital interests of the data subject;
- for the administration of justice pursuant to an order of the court of competent jurisdiction;
- for legitimate interests pursued by the data controller; or
- for the exercise of any functions conferred on any person by or under any law.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

Sensitive personal data may be processed based upon explicit consent of the data subject.

Apart from processing based upon explicit consent, the sensitive personal data may be processed based on 'necessity'. The draft Bill provides that sensitive personal data can only be processed if the processing is necessary:

- to exercise or perform any right or obligation that is conferred or imposed by law on the data controller in connection with employment;
- to protect the vital interests of the data subject or another person, in a case where:
  - consent cannot be given by or on behalf of the data subject; or
  - the data controller cannot reasonably be expected to obtain the consent of the data subject;
- to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- for medical purposes and is undertaken by:
  - a healthcare professional; or
  - a person who in the circumstances owes a duty of confidentiality that is equivalent to that which would arise if that person were a healthcare professional;
- for, or in connection with, any legal proceedings;
- to obtain legal advice while ensuring its integrity and secrecy;
- to establish, exercise or defend legal rights;
- for the administration of justice pursuant to orders of a court of competent jurisdiction; or
- for the exercise of any functions conferred on any person by or under any written law.

Sensitive personal data can also be processed if the information contained in the data has been made public as a result of steps deliberately taken by the data subject.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

A data controller shall, by written notice, inform a data subject:

- that personal data of the data subject is being collected and a description of the personal data;
- on the legal basis for the processing of personal data;
- on the duration for which personal data is likely to be processed and retained thereafter;
- on the purpose for which the personal data is being collected or is to be collected and further processed;
- on the information of the source of the personal data (if available with the data controller);
- on the data subjects' right to request access and correction of personal data and how to contact the data controller concerning any inquiries or complaints;
- on the class of third parties to whom the data controller discloses or may disclose the personal data;
- on the choices and means the data controller offers to the data subject for limiting the processing of personal data;
- whether it is obligatory or voluntary for the data subject to supply personal data; and
- where it is obligatory to supply personal data, the consequences on the data subject for failure to do so.

Notice is required to be given:

- when the data subject is first asked by the data controller to provide his or her personal data;
- when the data controller first collects the personal data of data subject;
- before the data controller uses the data subject's personal data for a purpose other than the purpose for which it was collected;
- before the data controller discloses the personal data to a third party; and
- in the national and English languages, and the individual (data subject) be provided with a clear and readily accessible means to exercise his or her choice.

Exemptions from transparency obligations

15 | When is notice not required?

Notice is not required to be given in the case the personal data is processed for:

- the prevention or detection of crime or for investigations;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax or duty or any other imposition of a similar nature;
- preparing statistics or carrying out research (provided that resulting statistics or results of the research are not made available in a form which identifies the data subject);
- the connection with any order or judgment of a court;
- the discharging of regulatory functions (if the application whereof would be likely to prejudice the proper discharge of those functions); and
- journalistic, literary or artistic (subject to certain conditions).

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

The Personal Data Protection Bill 2021 (the draft Bill) requires that a data controller is to take reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up to date by having regard to the purpose including any directly related purpose for which personal data was collected and further processed.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The draft Bill requires that processed personal data must be adequate and not excessive in relation to the lawful purpose for which it is collected.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The draft Bill requires that personal data processed for any purpose must not be kept longer than is necessary for the fulfilment of that purpose. The data controller is required to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The draft Bill (while discussing the general requirements for collection and processing of personal data) requires that personal data shall not be processed unless the processing is necessary for, or is directly related to, a lawful purpose directly related to an activity of the data controller (purpose limitation principle).

The purpose limitation principle is envisaged in the draft Bill. Presence of a lawful purpose directly related to the activity of the data controller is one of the underlying general principles governing the processing of personal data. In the case of use of the personal data for any other purpose, the data controller must give fresh notice to the data subject.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The draft Bill provides a right to the data subject not to be subjected to a decision solely based on automated processing including profiling.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Personal Data Protection Bill 2021 requires that a data controller or a data processor while processing the personal data, are to take practical steps to protect the personal data following the security standards prescribed by the National Commission for Personal Data Protection of Pakistan (the Commission). The Commission, considering the national interest, is to prescribe the best international standards to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

In the event of a personal data breach the data controller is to:

- notify the Commission and the data subject in respect of the breach;
- notify without any delay and not beyond 72 hours; and
- give reasons for the delay in the case the notification is made beyond 72 hours.

An exception to the above is where the breach is unlikely to result in a risk to the rights and freedoms of the data subject.

Information to be provided in the personal data breach notification includes:

- the description and nature of the personal data including (where possible) the categories and approximate number of concerned data subjects, and the categories and approximate number of concerned personal data records;
- the name and contact details of the data protection officer or another contact from where more information can be obtained;
- the likely consequences of the breach; and
- the measures adopted or proposed to be adopted by the data controller to address the breach.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Data controllers and data processors are to take practical measures to protect personal data in accordance with the security standards prescribed by the National Commission for Personal Data Protection of Pakistan (the Commission).

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There is no expressed requirement in the Personal Data Protection Bill 2021 (the draft Bill); however, while discussing the power of the Commission, the draft Bill confers upon it the power to formulate responsibilities of the Data Protection Officer. Therefore, the Commission, when established, will devise the appointment requirements.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The draft Bill requires that a data controller is to keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed. The Commission may determine the manner and form in which such record is to be kept.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The draft Bill does not specifically provide for any risk assessment. However, while discussing the powers of the Commission, the draft Bill empowers the Commission to formulate a compliance framework concerning data protection impact assessment. It follows that on establishment of the Commission, the Commission may frame rules as to when and to whom data protection impact assessment applies.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The draft Bill has no provisions regarding the design of processing systems.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no expressed requirement in the Personal Data Protection Bill 2021 (the draft Bill); however, while discussing the powers of the National Commission for Personal Data Protection of Pakistan (the Commission), the draft Bill confers upon it the power to devise a registration mechanism for data controllers and data processors. Therefore, the Commission, when established, will devise the registration requirements.

Other transparency duties

29 | Are there any other public transparency duties?

There are no such duties under the draft Bill.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

In such cases, the data controller is to ensure that the data processor undertakes to adopt applicable technical and organisational security standards governing the processing of personal data as prescribed by the National Commission for Personal Data Protection of Pakistan (the Commission). In addition, the processor itself is responsible for ensuring compliance with the security standards prescribed by the Commission.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The Personal Data Protection Bill 2021 (the draft Bill) requires that personal data without the consent of the data subject must not be disclosed for any purpose other than the purpose for which the same was to be disclosed at the time of collection. The personal data shall not be disclosed to any party other than a third party already notified to the data subject.

The draft Bill further provides that personal data may be disclosed for any purpose other than the purpose for which it was to be disclosed at the time of its collection in following circumstances:

- when the disclosure is necessary for the purpose of preventing or detecting a crime or for the purpose of investigation;
- when the disclosure is required or authorised by law or by order of a court;
- when the data collector acted in reasonable belief that he or she had in law the right to disclose;
- when data collector acted in reasonable belief that he would have had the consent if the data subject had known the circumstances of disclosure; or
- when disclosure was justified as being in the public interest in circumstances as determined by the Commission in advance of disclosure.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The draft Bill states that personal data may be transferred outside Pakistan in following cases:

- there is equal protection for the data in the foreign jurisdiction;
- the transferor has the consent of the data subject; and
- it is transferred under a framework to be devised by the Commission.

The draft Bill further provides that:

- critical personal data is not be transferred outside Pakistan; and
- the Commission must devise a mechanism to keep some components of sensitive personal data in Pakistan (data localisation of sensitive personal data).

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The Commission is empowered to devise a framework under which personal data may be transferred outside Pakistan. Once the

Commission is established, the framework related to the transfer of personal data outside Pakistan will be devised.

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

The draft Bill requires that some components of the sensitive data (that is transferred outside Pakistan) be kept locally in Pakistan (data localisation) based upon a mechanism to be devised by the Commission.

RIGHTS OF INDIVIDUALS

Access

35 Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

The Personal Data Protection Bill 2021 (the draft Bill) confers the right on the data subject to have access or a copy of his or her personal data held by the data controller. The data subject on payment of a prescribed fee makes a request in writing to the data controller. A data controller may refuse to comply with the request on the following grounds:

- the data controller is not supplied with such information as the data controller may reasonably require;
- the data controller cannot comply with the request without disclosing personal data relating to another individual who can be identified from that information;
- any other data controller controls the processing of personal data to which request relates in such a way as to prohibit the first-mentioned data controller from complying;
- providing access may constitute a violation of an order of a court;
- providing access may disclose confidential information relating to the business of the data controller; and
- access to personal data is regulated by another law.

Other rights

36 Do individuals have other substantive rights?

The draft Bill confers the following rights on the data subjects:

- the right to correct personal data;
- the right to withdrawal of consent;
- the right to prevent processing likely to cause damage or distress;
- the right to erasure;
- the right to data portability; and
- the right not to be subjected to a decision solely based on automated processing including profiling.

Compensation

37 Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The draft Bill does not provide for any damages or compensation to the data subjects.

Enforcement

38 Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Rights to the data subjects are to be enforced by the National Commission for Personal Data Protection of Pakistan (the Commission). Any decision or order of the Commission is appealable before the High Court or before a tribunal established by the federal government in the manner prescribed by the High Court.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 Does the law include any derogations, exclusions or limitations other than those already described?

The Personal Data Protection Bill 2021 (the draft Bill) applies to all sectors and types of organisations. However, it provides an exemption to specific processing from a few specified requirements, as follows:

- the prevention or detection of crime or for investigations;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax or duty or any other imposition of a similar nature;
- preparing statistics or carrying out research (provided that resulting statistics or results of the research are not made available in a form that identifies the data subject);
- the connection with any order or judgment of a court;
- the discharging of regulatory functions (if the application whereof would be likely to prejudice the proper discharge of those functions); and
- journalistic, literary or artistic (subject to certain conditions).

The above-stated are exempted from the following requirements:

- the general requirements (of lawful purpose, purpose limitation, data minimisation and consent);
- notice to the data subject;
- non-disclosure; and
- adherence to the security standards prescribed by the Personal Data Protection Authority of Pakistan (the Commission).

Also, the processing concerning the physical or mental health of data subject is exempted from the applicability of security standards prescribed by the Commission if application whereof would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

The draft Bill is not applicable on personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 Are there any rules on the use of 'cookies' or equivalent technology?

The Personal Data Protection Bill 2021 (the draft Bill) does not have any rules regarding the use of cookies. However, the data subject is given a right to not to be subjected to a decision solely based on automated processing including profiling.

Electronic communications marketing

41 Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Pakistan Telecommunication Authority (PTA) issued the Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations 2009 (the Regulations). The Regulations apply to all telecoms operators licensed by the PTA to ensure and protect the interests

of telecom consumers by preventing them from sending spam and fraudulent, unsolicited and obnoxious communication.

The Regulations require all operators to establish standard operating procedures to control spamming, fraudulent communication, unsolicited calls and obnoxious calls. The operators are also required to establish a Do Not Call Register in connection with controlling unsolicited calls. The operators are also required to ensure registration of telemarketers.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no rules in this regard. The draft Bill only provides a right for the data subject not be to subject to a decision solely based on automated processing including profiling.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Sensitive personal data may be processed based upon explicit consent of the data subject.

Apart from processing based upon explicit consent, the sensitive personal data may be processed based upon 'necessity'. The draft Bill provides that sensitive personal data can only be processed if the processing is necessary:

- to exercise or perform any right or obligation that is conferred or imposed by law on the data controller in connection with employment;
- to protect the vital interests of the data subject or another person, in a case where:
  - consent cannot be given by or on behalf of the data subject; or
  - the data controller cannot reasonably be expected to obtain the consent of the data subject;
- to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- for medical purposes and is undertaken by:
  - a healthcare professional; or
  - a person who in the circumstances owes a duty of confidentiality that is equivalent to that which would arise if that person were a healthcare professional;
- for, or in connection with, any legal proceedings;
- to obtain legal advice while ensuring its integrity and secrecy;
- to establish, exercise or defend legal rights;
- for the administration of justice pursuant to orders of a court of competent jurisdiction; or
- for the exercise of any functions conferred on any person by or under any written law.

Sensitive personal data can also be processed if the information contained in the data has been made public as a result of steps deliberately taken by the data subject.

Profiling

44 | Are there any rules regarding individual profiling?

There are no rules in this regard. The draft Bill only provides a right to data subject to not to subject to a decision solely based on automated processing including profiling.

S.U.Khan Associates
Corporate & Legal Consultants

Saifullah Khan
saifullah.khan@sukhan.com.pk

Saeed Hasan Khan
saeed.hasan@sukhan.com.pk

First Floor, 92-Razia Sharif Plaza
Fazal-ul-Haq Road
Blue Area
Islamabad (44000)
Pakistan
Tel +92 51 2344741
Fax +92 51 2344743
www.sukhan.com.pk

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The government's Digital Pakistan Policy sets the goals and directions for the Internet of Things, fintech, artificial intelligence and robotics, cloud computing and big data. However, there is no law or regulation at present. The Securities and Exchange Commission of Pakistan has issued the draft Cloud Adoption Guidelines for Incorporated Companies/ Business Entities. The draft Guidelines treat 'personally identifiable information' (PII) as sensitive official data. As per the draft Guidelines, the PII is any data that could potentially be used to identify a particular person. The draft Guidelines require that, in the case of PII, only the most secure cloud service providers should be relied upon. The Guidelines further require that business entities must encrypt PII and ensure that the key and encrypted PII is not stored on same cloud.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Ministry of Information Technology and Telecommunication (government of Pakistan) set out plans in the National Cyber Security Policy 2021. One of the significant aspects of the policy is to create the Cyber Security Act and develop rules and regulations for the national cybersecurity framework. The Ministry of Information Technology and Telecommunication is expected to commence the drafting of the Cyber Security Act.

Poland

Marcin Lewoszewski, Anna Kobylańska and Arwid Mednis

Kobylańska Lewoszewski Mednis

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

As Poland is a member of the European Union, the Polish legislative framework related to protection of personal data arises mostly from EU regulations and directives. The General Data Protection Regulation (GDPR) is a key element of that framework, surrounded by sector-specific regulations. In addition, Poland enacted the Data Protection Law of 2018 that regulates selected operational aspects of data protection (eg, functioning of the Polish Data Protection Authority (DPA) or notification of the designation of data protection officer to the mentioned authority).

There is a number of sector-specific regulations with elements of data protection law, including banking law, insurance law, telecommunications law and the Labour Code, among others.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The DPA is a single authority in Poland responsible for overseeing data protection law. It is authorised to conduct formal proceedings and inspections. The inspections are, in practice, conducted by inspectors of the DPA, who are authorised to:

- enter, from 6am to 10pm, the grounds and buildings, premises or other rooms of the inspected entity;
- access documents and information directly related to the objective scope of the inspection;
- carry out inspections of places, objects, devices, carriers and IT systems used for data processing;
- demand the submission of written or oral explanations and question the person as a witness to the extent necessary to establish the actual state of affairs; and
- commission the preparation of expert opinions and opinions.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The DPA is required to cooperate with other supervisory authorities in line with Chapter VII of the GDPR. This is often the case in relation to processing of personal data by controllers operating across the EU or globally.

If the DPA receives a motion from a supervisory authority of another EU member state regarding participation in a joint operation referred to in article 62 section 1 of the GDPR, or the DPA submits such a request, the DPA shall make arrangements with the supervisory authority of another EU member state regarding the joint operation.

In practice, the DPA is actively involved in cross-border cooperation with other authorities, including taking part in cross-border proceedings related to the GDPR non-compliance.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection law can lead to administrative sanctions or orders, as well as – in some cases –criminal sanctions. The DPA is active in the field of sanctioning, in particular in relation to personal data breaches.

Proceedings before the DPA are formal and are based on administrative law. Each proceeding should be finished by issuing a binding decision that can be questioned before the administrative court in Warsaw.

1.5 Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Yes, controllers may appeal against orders of the supervisory authority within 30 days of receiving an order.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Generally, only processing of personal data for purely personal or household activity, as well as the processing of data of deceased persons, is outside the scope of the Data Protection Law of 2018 and the General Data Protection Regulation (GDPR). In other cases, the GDPR and Polish law apply to private and public sector bodies.

The Act of 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime regulates processing data on this purpose.

The processing of data by the Catholic Church is regulated separately in the Act on General decree on the protection of individuals with regard to the processing of personal data in the Catholic Church.

Polish provisions of data protection law may also limit or exclude the application of certain obligations of controllers, such as the obligation to inform individuals about collecting and using their data or to ensure the exercise of their other rights (eg, the right of access and the right to data erasure).

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Electronic marketing is regulated by the Polish act on the provision of services by electronic means, which implements the EU E-commerce Directive (Directive 2000/31/EC of 8 June 2000). Marketing phone calls are regulated by the Polish Telecommunication Law.

The eavesdropping and interception of communication are regulated by 'police acts' (ie, the acts that regulate the operations of police and other special forces) and in the Code of Criminal Procedure. Also, Polish Telecommunication Law provides some obligations for the operators of a public telecommunications network and providers of publicly available telecommunications services concerning data generated in the telecommunications network (eg, the obligation to store the data and make it available at the request of authorised special forces).

In Polish law, there is no general regulation on monitoring. Specific regulations are provided in several acts, for instance, employee monitoring is regulated in Labour Law Code.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

There are numerous legal acts that provide specific data protection rules for related areas.

For instance, employee monitoring is regulated in the Labour Code, and monitoring in entities performing medical services is regulated in Healthcare Institutions Law. The Labour Code and several acts concerning employees (eg, law on company social benefits fund) provide some specific rules on the processing of employees' data.

The processing of debt information is regulated by the act on the provision of economic information and the exchange of economic data. Further provisions in this area may be found in the Banking Law.

PI formats

9 | What categories and types of PI are covered by the law?

The GDPR provides the definition of personal data, which is any information relating to an identified or identifiable natural person. The identifiable person means the one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Generally, Polish law does not distinguish PI based on the format of the data. However, the GDPR covers PI processed in electronic form (the processing wholly or partly by automated means) and PI processed in a non-electronic form, which form a part of a filing system or are intended to form part of a filling system.

The decision as to whether PI form or are intended to form a filing system must be considered on a case-by-case basis.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The GDPR applies to:

- controllers and processors established in the European Union, even if the processing does not take place in the EU; and
- controllers and processors that are not established in the EU, if data subjects are in the EU and the offering of goods or services is directed to these data subjects or if the monitoring of data subjects takes place within the EU.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The GDPR covers PI processed in electronic form (the processing wholly or partly by automated means) and PI processed in a non-electronic form, which form part of a filing system or are intended to form part of a filing system – other types of processing are not covered.

The GDPR applies to controllers (entities or persons that determine purposes and means of processing personal data) and processors (entities or persons that process personal data on behalf of the controller).

As the controller decides on the scope and the purposes of processing the data, the primary obligations lie with the controller. Processors may only act on the instructions of the controller. Their duties mainly consist of supporting the controller (eg, processors must assist in ensuring compliance with the controllers' obligations considering the cooperation with a supervisory authority or with data subjects' requests).

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes, the General Data Protection Regulation requires that personal data be processed lawfully.

Processing must be lawful only if and to the extent that at least one of the following applies:

1 the data subject has given consent to the processing of his or her personal data;
2 processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
3 processing is necessary for compliance with a legal obligation to which the controller is subject;
4 processing is necessary to protect the vital interests of the data subject or of another natural person;
5 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; and
6 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 protection of personal data, in particular where the data subject is a child.

Point (6) shall not apply to processing carried out by public authorities in the performance of their tasks.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Yes, the law imposes more stringent rules for special categories of personal data which include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing of such special categories of personal data is prohibited unless one of the following applies:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- 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 and social security and social protection law in so far as it is authorised by EU or member state law or a collective agreement pursuant to member state law;
- 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;
- 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;
- processing relates to personal data that is manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of EU or member state law;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, 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 EU or member state law or pursuant to contract with a health professional;
- 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 EU or member state law; and
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EU or member state law.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Yes. Controllers, according to articles 13 and 14 of the General Data Protection Regulation (GDPR), are obliged to inform data subjects about:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on legitimate interests of a controller or a third party, the legitimate interests pursued by the controller or by the third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission, as well as reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

When the personal data has not been obtained from the data subject, the controller must also inform individuals of the source from which the PI originated and the categories of PI obtained.

The information must be provided when personal data is obtained. When PI is obtained from a source other than the data subject, the controller must provide the required information in a reasonable period after obtaining the PI and no later than one month. The general time limit of one month may be further curtailed, where the data is being used for the communication with the data subject or where the data is being disclosed to another recipient. In such cases, the information must be given at the latest at the time of the first communication or at the latest at the time of the first disclosure.

Exemptions from transparency obligations

15 | When is notice not required?

The controller is not obliged to inform the data subject if the data subject already has the information. Additionally, when the data has not been obtained from the data subject, the notice is not required when:

- the provision of such information would be impossible or require disproportionate effort;
- the provision of such information is likely to render impossible or seriously impair the achievement of the objectives of the processing;
- obtaining or disclosure is expressly laid down by EU or member state law; and
- the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or member state law.

Data accuracy

16 Does the law impose standards in relation to the quality, currency and accuracy of PI?

The controller must ensure that PI is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; 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.

Data minimisation

17 Does the law restrict the types or volume of PI that may be collected?

Yes. PI must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. The data protection regulations do not regulate specific volumes of data that can be processed but may impose some additional obligations in relation to large-scale data processing, such as the need to carry out a data protection impact assessment. Concerning the type of data, there are restrictions when it comes to the bases for data processing (eg, special categories of data), but these restrictions are not of a quantitative nature.

Data retention

18 Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

PI must be kept for no longer than is necessary for the purposes for which the personal data is processed. The Polish Data Protection Act of 2018 and the GDPR do not impose any specific retention periods; however, the retention periods are sometimes provided in specific laws such as civil law or tax law. There are cases where the Polish law provides with a closed catalogue (list) of data that can be collected from data subjects, as well as with specific retention periods.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Where the controller intends to further process the personal data for a purpose other than that for which it was collected, prior to that further processing, the controller must provide the data subject with information on that other purpose and any relevant further information.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Sometimes, specific provisions (eg, the Payment Services Act) may provide for a limitation of the purposes of the processing. Consequently, the possibility of using PI for a new purpose must be assessed on a case-by-case basis.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Yes. Any decision based solely on automated processing, including profiling, which produces legal effects concerning data subjects or similarly significantly affects data subjects, falls under specific restrictions:

- it is necessary to obtain a legal basis for doing so (there is explicit consent, under the performance of a contract with the data subject or as authorised by law);
- it is necessary to inform data subjects about automated decision-making;
- specific technical or organisational measures must be implemented addressing the risks involved in such data processing operations;
- data subjects must have the right to obtain human intervention; and
- data subjects must have the opportunity to express their points of view and to contest the decision.

This includes automated processing of PI and the use of PI to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning, for example, performance at work, economic situation, behaviour, location and movements.

Sometimes, specific provisions authorising automated decision-making (eg, banking law) may provide for certain additional restrictions (eg, a catalogue of data that may be processed).

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Polish Data Protection Act of 2018 does not contain any additional requirements regarding the security of personal data in relation to the General Data Protection Regulation (GDPR). Controllers and processors are therefore obliged to apply general principles, resulting in particular from article 32 of the GDPR. Some sectoral legislation, for example, on administrative enforcement, housing or state archives, contains some additional data security requirements. These additional requirements include the restriction of access to data, the obligation to test systems and others.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The general principles of notifying data breaches and informing data subjects about data breaches arise from articles 33 and 34 of the GDPR and in the case of entities from electronic communications sector, from Commission Regulation No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications. Polish sectoral regulations generally do not exclude or amend the rules resulting from the GDPR, but only in some cases indicate the authorities that are entitled to establish more detailed rules for reporting data breaches.

Controllers are obliged to notify a personal data breach (ie, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed to the data protection authority). There is no materiality threshold, however the controller is exempted from the notification obligation if the breach is unlikely to result in a risk of the rights and freedoms of natural persons. When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subject should also be notified. Notification to the DPA should take place within 72 hours of having become aware of the breach, and notification to data subjects should be provided without undue delay.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The controller or processor shall be responsible for, and must be able to demonstrate compliance with, all the principles stated in the General Data Protection Regulation (GDPR). There are no specific rules on the demonstration of accountability, but individual obligations, such as keeping a record of processing activities, are a way to demonstrate compliance with the law.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The appointment of a data protection officer is mandatory in the following cases:

- the core activities of the controller or processor consist of processing operations that, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- the main activities of the controller or processor consist of processing on a large scale special categories of personal data and personal data relating to criminal convictions and offences; and
- the processing is carried out by a public authority or body (with the exception of courts in the exercise of their judicial functions).

The data protection officer is expected to play a key role in fostering a 'data protection culture' and to help implement the necessary requirements of the GDPR. The data protection officer must have at least the following tasks and responsibilities:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations;
- to monitor compliance with the GDPR, with other EU or member state data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authority; and
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Yes, the controllers and the processors are obliged to keep and maintain the following records:

- a record of processing activities (for controllers) and a record of all categories of processing activities (for processors); and
- a register of personal data breaches.

In addition, controllers and processors may be indirectly required to maintain appropriate records and documentation to the extent that this will enable them to demonstrate compliance with the provisions of the GDPR. For example, procedures for the exercise of data subjects' rights or maintaining a register of data processing entrustment agreements may be relevant documentation. However, the keeping of such registers or documentation is not explicitly required by law.

Risk assessment

26 Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Yes, certain processing operations should be subject to a data protection impact assessment. It is required whenever processing operations are likely to present a high risk of harming the rights or freedoms of natural persons. It is necessary at least in the following situations:

- making a systematic, comprehensive assessment of individuals' personal factors, including on the basis of profiling;
- large-scale processing of special categories of data; and
- systematic large-scale monitoring of publicly accessible places.

National DPAs, together with the European Data Protection Board (EDPB), may make available a list of cases where a data protection impact assessment will be required. The impact assessment should be carried out before the start of processing operations and should be treated not as a one-off study but as an evolving process.

The Data Protection Authority has provided a list of the types of personal data processing operations that require an assessment of the effects of processing on data protection, among which are, inter alia:

- automated decision-making with legal, financial or similar significant effects;
- processing of genetic data; and
- processing of location data.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Controllers already at the stage of determining the means of processing, as well as during the processing itself, are required to apply the principle of privacy by design (ie, to implement appropriate technical and organisational measures, such as pseudonymisation), designed to effectively implement data protection principles, such as data minimisation, and to give the processing the necessary safeguards. The core of this approach is the application of the principle of minimisation (ie, PI must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed). The guidelines adopted by the EDPB should also be taken into account while applying the principles of privacy by design and privacy by default (eg, the guidelines regarding transparency or dark patterns).

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

In Poland, there is no obligation for controllers and processors to register with the Data Protection Authority (DPA).

They only have an obligation to notify the DPA of the designation of a data protection officer (DPO). This obligation must be fulfilled within 14 days of the date of the officer's appointment. The general rules on penalties apply in the event of failure to notify the DPO.

The above also applies if the entity has appointed a person to replace the data protection officer during his or her absence.

Other transparency duties

29 | Are there any other public transparency duties?

The entity that designated the DPO provides the officer's data immediately after his or her appointment, on its website, and if it does not run its own website, in a manner generally available at the place of business.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The transfer of PI to entities that provide outsourced processing services is regulated in the General Data Protection Regulation (GDPR). If such entity processes PI on behalf of the controller, it is considered to be a data processor. The controller is responsible for selecting a processor that provides sufficient guarantees to implement appropriate technical and organisational measures. This means that the processor has to meet the requirements of the GDPR and ensure the protection of the rights of the data subjects. Such outsourcing has to be governed by a in writing (including electronic form) or other legal act. The contract has to contain the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller as well as stipulate, in particular, that the processor:

- processes the personal data only on documented instructions from the controller;
- ensures that persons who will process PI are subject to a confidentiality obligation;
- implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk;
- obtains authorisation before appointing sub-processors and ensures that that sub-processors are bound by the same data protection obligations as set out in the contract between the controller and the processor;
- assists the controller in ensuring compliance with the obligations regarding data subjects and supervisory authorities;
- at the choice of the controller, deletes or returns all the PI after the provision of services;
- immediately notifies the controller if in its opinion any instruction given by the controller infringes the GDPR; and
- makes available to the controller all information necessary to demonstrate compliance with the above obligations, and allows the controller (or another auditor mandated by the controller) to carry out an audit.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

In some branches and professions, there are professional secrecies regulated by specific acts that limit the possibility of disclosing information, including information containing personal data. These include, among others, banking secrecy, insurance secrecy, telecommunications secrecy, attorney–client privilege and doctor–patient confidentiality.

Disclosure of data to any person acting under the authority of the controller (such as employees) or of the processor must be done under the condition that such person will process data on instructions from the controller (unless required to do so by the law).

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The transfer of PI outside the European Economic Area is restricted. Such transfer is permitted when:

- the EU Commission has decided that – for example, the third country or the international organisation – ensures an adequate level of protection;
- appropriate safeguards are provided, such as Standard Contractual Clauses or Binding Corporate Rules and simultaneously data subject rights are enforceable and effective legal remedies for data subjects are available; and
- specific situations occur (and such a transfer is an exception), for example, on the basis of the data subject's explicit consent or if the transfer is necessary for the performance of a contract between the data subject and the controller or if it is necessary to establish, exercise or defend legal claims.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The data processing provisions set in the GDPR, together with transfer restrictions, are equally binding for controllers and processors, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. In all cases, transfers to third countries and international organisations may only be carried out only in full compliance with the GDPR.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No, there is no such general requirement for PI, but it is necessary in certain cases to inform the data subject of the place of data storage in a third country.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

All individuals who are data subjects, in principle, have the right of access to their PI from the PI owner (controller) in readily understandable form.

In general, the controller has one month to satisfy the request or reply stating that he or she does not process data of the applicant. When fulfilling a request, the controller should use all reasonable measures to verify the identity of a data subject who requests access.

Like most of the rights of the data subject, the right of access also can be restricted by EU or member state law. Restrictions must respect the essence of the fundamental rights and freedoms and be necessary and proportionate measure in a democratic society to safeguard one of public interests, listed in article 23 of the General Data Protection Regulation (GDPR).

Examples of restrictions on the right of access include:

- financial entities in regard to anti-money laundering duties and crime prevention;
- partial restriction with regard to subjects of administrative procedure;
- advocacy, bailiff and tax consultant confidentiality;
- partial restriction with regard to cooperative law;
- data related to prosecution of environmental crimes by the Environmental Protection Inspection;
- processing of data by the Bureau of Statistics;
- private detective operations;
- processing of data for the purpose of scientific research, when it is necessary; and
- other situations where the restriction is imposed to safeguard rights, freedoms safety or prevent crime.

Requesting information more than once can be subjected to fee based on administrative costs incurred by controller.

Other rights

36 | Do individuals have other substantive rights?

Yes, other rights include the:

- right to withdraw consent at any time, except where consent does not constitute the basis for the processing;
- right of rectification;
- right of erasure (the right to be forgotten);
- right of restriction of processing;
- right to object to processing;
- right to data portability;
- in the case of automated decision-making, right to obtain human intervention, the right to express opinions and the right to contest the decision;
- right to lodge a complaint to Data Protection Authority (DPA); and
- right to compensation.

Some of the above mentioned rights are limited by the GDPR and can be further restricted by EU or member state law.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes, the GDPR formulates the principle of full compensation. A person may claim actual loss (*damnum emergens*) or lost profits (*lucrum cessans*), as well as compensation for non-material damage related to the violation of intangible goods.

If damage occurs, the controller is presumed to be at fault until he or she proves that he or she is in no way responsible for the event giving rise to the damage.

If the event results in breach of personal rights, for example right to privacy, the right to protection of a name and pseudonym or the right to personal portrayal, the individual may also be entitled to monetary damages or compensation under article 24 of the Polish Civil Code.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The right to compensation is exercisable through the judicial system. All other personal rights regarding data subjects are enforced by the supervisory authority – the DPA. To enforce those rights, the DPA has power to:

- issue warnings and reprimands;
- order to comply with the data subject's requests;
- order to bring processing operations into compliance with the GDPR;
- 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 and the notification of such actions to people affected;
- withdraw a certification;
- impose an administrative fine; and
- order the suspension of data flows outside EU.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

The limitations to the application of the General Data Protection Regulation (GDPR) are included in the GDPR itself as well as in Polish law. The Polish Data Protection Act of 2018 limits or excludes the application of the GDPR in full or certain obligations of the controller for specific purposes or entities, such as, an obligation to inform individuals about collecting and using their data or to ensure the exercise of their other rights. Various limitations and exclusions concern:

- processing for academic purposes;
- statement as a part of a literary or artistic activity;
- processing for journalistic purposes (editing, preparing, creating and publishing press materials);
- processing for the performance of a task carried out in the public interest (if the fulfilment of the obligation prevents or seriously impairs the proper performance of the task and the rights and freedoms of the individual do not override the interest resulting from the performance of the task); and

- processing by certain units of the financial public sector (if the processing is necessary to safeguard national security and the law stipulates necessary measures for ensuring the protection of the individual's rights and freedoms).

Although the GDPR generally applies to data processed by religious institutions, the processing of personal data by the Catholic Church is regulated separately in the Act on General decree on the protection of individuals with regard to the processing of personal data in the Catholic Church.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

In general, storing information or accessing information already stored in the telecommunications terminal equipment of a subscriber or end user is permitted provided that the subscriber and end user:

- is directly informed (in an unambiguous, easy and understandable manner) of the purpose of storing as well as of the possibility of modifications in storing or accessing the information (via internet browser);
- gives his or her consent to it (under the conditions provided for consent in the data protection regulations); or
- the stored information or access does not cause configuration changes in telecommunications terminal equipment and the software.

Consent is not required if the information is used only for the transmission of communications over a public telecommunications network or is necessary to provide a service requested by the subscriber or end user.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

It is unlawful to send unsolicited commercial communications by electronic means (in particular via SMS or email) or make unsolicited marketing phone calls (including automated calling systems). To send electronic marketing or make marketing phone calls, the entity must gain opt-in consent. The consent must meet the requirements provided by the data protection regulations. The consent may be given by the subscriber directly or – indirectly – by providing an email address that identifies him or her (to obtain commercial information).

In terms of data processing, generally the legal basis for marketing purposes is consent or legitimate interest of the controller or third party.

Targeted advertising

42 | Are there any rules on targeted online advertising?

Yes, besides the general restrictions inherent in the advertising sector as a whole, online advertising is subject to a number of regulations, mainly concerning the grounds for using tracking technologies such as cookies or beacons, as well as the legal grounds for sending unsolicited commercial communications by electronic means. Further, the restrictions also cover the profiling of data subjects and the automated decision-making that have legal effect or similarly significantly affect the data subject.

An essential requirement to carry out targeted online advertising is to obtain valid consent to carry out such activities or to identify other legal bases, if applicable.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The term 'sensitive' data in Poland refers to 'special' categories of data, the processing of which is by default prohibited, unless the enumerated circumstances apply. Special categories of data are those revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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.

The special categories of data may be processed, when one of the following applies:

- the data subject has given explicit consent to the processing of this personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by law or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- 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;
- 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 the 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;
- processing relates to personal data that is manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care, or the treatment or the management of health or social care systems and services;
- 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 health care and of medicinal products or medical devices; and
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Profiling

44 | Are there any rules regarding individual profiling?

Profiling, as a form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, is in principle not regulated. However, if it results in automated decision-making (ie, there is no human involvement in the individual decision-making process), the restrictions provided for automated decision-making apply. Profiling, which does not constitute automated decision-making nor does it produce legal effects or similarly affect the data subject, is subject to general principles relating to the processing of personal data.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There is no law in Poland applicable specifically to providing cloud computing. The provision of cloud computing services is covered by generally applicable laws, mainly civil contract law, consumer protection law, provision of services by electronic means, data protection and cybersecurity.

Special security and geohosting requirements may apply when services are provided to Polish public administration entities through the ZUCH platform (Cloud Service Delivery System). Personal data and company secrets will have to be hosted in a Polish jurisdiction and will require a higher standard of data safety (on the level of Cyber Security Standards for Cloud Computing 2), while services that do not require processing any restricted data can be provided from the territory of EU member states. Specific requirements are also provided for entities from the banking sector, for example, by the Polish Financial Supervision Commission or the the European Banking Authority in their guidelines on outsourcing.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

It is likely that in the next months the new ePrivacy Act will be in the spotlight, and significant legislative progress or even adoption can be expected. Other legislative initiatives under the Digital Single Market Strategy for Europe may be finalised, including regulations in the pipeline to complement privacy-related regulations such as the Data Governance Act, the Digital Services Act, the Digital Market Act or the the NIS 2 Directive.

We expect the Data Protection Authority to focus on the processes of securing and sharing personal data processed by processors related to the use of mobile applications, in particular on how to secure and share personal data processed in connection with the use of these applications. In addition, we expect that the supervisory authority will examine the processing of the personal data of bank clients and potential clients with respect to profiling. Moreover, the authority will check the ways in which credit applicants are informed about their creditworthiness assessment. As announced, the supervisory authority will also take action to verify the processing of personal data by processors in the Schengen Information System and the Visa Information System.

Marcin Lewoszewski
marcin.lewoszewski@klmlaw.pl

Anna Kobylańska
anna.kobylanska@klmlaw.pl

Arwid Mednis
arwid.mednis@klmlaw.pl

ul. Śniadeckich 10
00-656 Warsaw
Poland
Tel: +48 22 25 34567
www.klmlaw.pl/en

Portugal

Helena Tapp Barroso and Tiago Félix da Costa

Morais Leitão, Galvão Teles, Soares da Silva & Associados

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The legislative framework for the protection of PI applicable in Portugal is (since 25 May 2018) that resulting from the direct application of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR).

National legislation providing for specific rules in the context of the GPDR is Law No. 58/2019 of 8 August 2019 (DPA). This law repealed the previous dedicated Portuguese data protection law governing personal data processing, issued in 1998 (Law No. 67/98 of 26 October 1998). A previous data protection law had been issued in 1991 (Law No. 10/91) dedicated to the protection of personal data processed by automated means. The initial law was based on the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data (Convention 108), adopted by the Council of Europe and Law No. 67/98, which transposed the provisions of Directive 95/46/EC (the Data Protection Directive).

Portugal has relevant national constitutional privacy provisions with article 35 of the Portuguese Constitution (on the use of computerised data) setting forth the main relevant principles and guarantees that rule PI protection.

International instruments relevant for PI protection have also been adopted in Portugal, including:

- Convention 108;
- the Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights), of which article 8 is specifically relevant for PI protection; and
- articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The National Commission for the Protection of Data (CNPD) is the supervisory authority responsible for overseeing the application of the data protection rules and principles in Portugal.

The CNPD (its members or delegated staff) have powers to require information on PI processing activities from public or private bodies and hold rights of access to the computer systems supporting PI processing, as well as to all documentation relating to the processing and transmission of PI, within the scope of its duties and responsibilities.

These include, among others, the responsibility to:

- supervise and monitor compliance with the laws and regulations regarding privacy and PI transfer;
- exercise investigative powers related to any PI processing activity, including PI transmission;
- exercise powers of authority, particularly those ordering the blocking, erasure or destruction of PI or imposing a temporary or permanent mandatory order to ban unlawful PI processing;
- issue public warnings or admonition towards PI owners failing to comply with PI protection legal provisions;
- impose fines for breaches of the DPA or other specific data protection legal provisions; and
- report criminal offences to the Public Prosecution Office in the context of the DPA and pursue measures to provide evidence thereon.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Cooperation between the supervisory authorities applicable to the Portuguese supervisory authority is currently subject to the provisions of Chapter VII, article 51(2) of the GDPR on cooperation and consistency, which states:

> *Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.*

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection law can lead to both administrative sanctions or orders and criminal penalties.

The administrative fines covering data protection law breaches under the GDPR apply. The DPA provides for specific rules in the context of the GPDR, including a complete chapter on administrative sanctions that contains provisions setting ranges of fines (minimum and maximum) and classifying infringements according to their nature and gravity, in line with article 83 of the GDPR. Different ranges are set for infractions incurred by individuals, small and medium enterprises and large undertakings (as defined in the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises).

Sector-specific legislation for the protection of PI in the electronic communication business activity (eg, applicable to PI owners that are telecom operators and internet service providers) foresee administrative fines for data protection law breaches that may go up to a maximum of €5 million.

Criminal offences are punished with fines or imprisonment ranging from six months to four years.

Administrative sanctions and orders are applied by the CNPD, which also has powers to order ancillary administrative measures such as temporary or permanent data processing bans or PI blockage, erasure or total or partial PI destruction, among others.

Criminal offences are subject to prosecution by the Public Prosecutor and their application must be decided by the criminal courts.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

PI owners can appeal to the courts against orders from the data protection authority, particularly from decisions of the data protection authority applying fines for infractions of GDPR or DPA provisions.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

All sectors and types of organisations are covered by Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and Law No. 58/2019 of 8 August 2019 (DPA) in their scope. The processing of PI by both public and private entities is covered by the GDPR and the DPA provisions and scope.

There is an applicable exemption, under the GDPR, for PI processing carried out by natural persons in the course of purely personal or domestic activities.

The provisions apply to the processing of personal data regarding public security, national defence and state security, without prejudice, however, to special rules contained in international legal instruments to which Portugal is bound, as well as specific domestic laws on the relevant areas.

The provisions of the DPA do not apply to the personal data files kept under the control of the Portuguese Intelligence System – a public entity that reports directly to the prime minister and cabinet and is responsible for providing support to policymakers on the evaluation of threats to the national interest, internal and external security, and the maintenance of the independence, unity and integrity of the Portuguese state – that is subject to specific legislation.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Several issues are covered by specific laws and regulations.

Video surveillance and surveillance cameras for defined purposes are the objects of specific laws, as is the case, among others, of:

- Law No. 51/2006 of 29 August 2006 on the setting up and operation of electronic surveillance systems on the roads for accident and incident prevention and management by highways agencies;
- Law No. 1/2005 of 10 January 2005 (subsequently amended and republished by Law No. 9/2012 of 23 February 2012) on the installation and use of surveillance through video cameras in public areas by national security forces (for the protection of public buildings, including premises of defence and security importance, people and asset security, crime prevention, driving infraction prosecution, prevention of terrorism and forest fire detection) and Decree-Law No. 207/2005 of 29 November 2005 specifically on electronic surveillance on the roads (eg, cameras and radars) by traffic police and other security forces; and
- Law No. 34/2013 of 16 May 2013 on the licensing of private security agencies and their activity, which contains relevant provisions on the use of video surveillance cameras (subsequently amended and republished by Law No. 46/2019 of 8 July 2019 and Ordinance No. 273/2013 of 20 August 2013, also subsequently amended by Ordinance No. 106/2015 of 13 April).

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

In Portugal, some sector-specific or purpose-specific provisions for the protection of PI may be found in specific laws or regulations. A relevant example of these are the rules specifically applicable to the electronic communications (telecom) sector contained in Law No. 41/2004 of 18 August 2004, which implemented Directive 2002/58/EC (the ePrivacy Directive) as amended by Law No. 46/2012 of 29 August 2012, implementing Directive 2009/136/EC (the Cookie Directive) (which also amended the ePrivacy Directive) and Commission Regulation (EU) No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under the ePrivacy Directive. The reform of ePrivacy legislation currently taking place in the European Union in line with the new rules in force under the GPDR will, no doubt, bring changes in this area to local legislation.

The provisions of Directive 2006/24/EC (the Data Retention Directive) amending the ePrivacy Directive have also been implemented in Portugal through Law No. 32/2008 of 17 June 2008 on the retention and transfer of such PI for the investigation, detection and prosecution of serious crime by competent authorities.

Another specific scope or sector acts may also be referred to, as is the case of Law No. 12/2005 of 26 January 2005 (as amended) and Decree-Law No. 131/2014 of 29 August 2014, both on personal genetic and health information.

The Portuguese Labour Code (2009) also contains several provisions on employee privacy, including provisions on monitoring and surveillance – namely, excluding the possibility of surveillance equipment being used by the employer to control employee performance (articles 20 to 22) and consultation requirements with employee work councils for certain types of processing. In the context of the coronavirus pandemic, specific provisions were also issued on the possibility of employee temperature measuring or covid-19 testing by employers.

Law No. 41/2004 of 18 August 2004, as amended by Law No. 46/2012 of 29 August 2012, which governs the processing of personal data and privacy in the electronic communications sector, contains specific provisions on unsolicited communications for marketing purposes.

PI formats

9 | What categories and types of PI are covered by the law?

The legislation applicable in Portugal covers PI processed by totally or partially automatic means as well as PI that forms part of a (manual) filing system or is intended to form part of such systems (the GDPR). PI refers to any information relating to an identified or identifiable natural person. The GDPR does not apply, as a rule, to the personal data of deceased persons but it foresees that member states may provide for rules regarding the processing of personal data of deceased persons.

The DPA includes a provision foreseeing that PI relating to deceased individuals is protected under the provisions of the GDPR and those of same DPA when consisting of special categories of data foreseen in article 9 of the GDPR (ie, genetic, biometric, health, sex life, sexual orientation, political opinions, trade union membership, religious or philosophical beliefs and racial or ethnic origin) or when it refers to private life PI or communication (traffic) data.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The DPA covers PI processing carried out in the context of the activities of an establishment of the PI owner located in Portuguese territory or in a place where Portuguese law applies by virtue of international public law.

Also covered is processing carried out by a PI owner established outside Portuguese territory affecting individuals (whose PI they process) who are in Portugal, where the processing activities are related to the offering of goods or services to such individuals in Portugal, irrespective of whether payment is required, or the monitoring of their behaviour as far such behaviour takes place within the Portuguese territory. The DPA provisions also apply to the processing of PI registered in Portuguese consulates regarding Portuguese individuals residing outside Portugal.

Nevertheless, the GDPR territorial scope, as defined in article 3, fully applies.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

All PI processing is covered regardless of whether it is processed by those who control or own PI or by those who provide PI processing services to owners. A significant number of duties apply both to controllers and processors, although some of the duties differ, in the sense that they apply to PI owners or, controllers, to use GDPR terminology.

All specific processor and controller duties resulting from the GDPR directly apply in Portugal. Administrative penalties and criminal infractions apply to the latter, while entities that process personal data on behalf of the controller (when in breach of specific processor legal duties or duties applicable to both processor and controller).

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The provisions contained in Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), particularly in articles 6 and 9 on the requirement that the holding of PI be legitimised on specific grounds, fully apply.

In line with article 6 of the GPDR, PI processing shall be lawful only if and to the extent that at least one of the following applies:

- the individual has given free, informed and unambiguous consent to the processing of his or her personal data for one or more specific purposes;
- the processing of the PI is necessary for the performance of a contract to which the individual is party or to take steps at the request of the latter before entering into a contract;
- PI processing is necessary for compliance with a legal obligation to which the PI owner (controller) is subject;
- PI processing is necessary to protect the vital interests of the individual or another natural person;
- PI processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; or
- PI processing is necessary for the legitimate interests pursued by the owner (controller) or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual that require protection of personal data, in particular where the individual is a child.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

More stringent rules apply in the case of the 'special categories of data' indicated in article 9 of the General Data Protection Regulation (GDPR). This refers to the PI processing of genetic, biometric, health, sex life, sexual orientation, political opinions, trade union membership, religious or philosophical beliefs and racial or ethnic origin and suspicion of illegal activities, criminal or administrative offences and decisions applying criminal penalties, security measures, administrative fines or additional conviction measures.

As a rule, the processing of special categories of PI is prohibited, with the exceptions provided for in article 9 of the GPDR. Currently, Law No. 58/2019 of 8 August 2019 (DPA) does not provide for any additional exceptions.

In the case of PI relating to health or sex life, including genetic data, the processing is also legitimate on medical grounds (eg, preventive medicine, medical diagnosis, provision of medical care and management of healthcare services).

The processing of information consisting of the suspicion of illegal activities or criminal or administrative offences is allowed on the grounds of pursuing the legitimate purposes of the PI owner, provided the latter is not overridden by the individual's fundamental rights and freedoms.

The processing of PI relating to criminal convictions and offences or related security measures shall be carried out only under the control of the official authority or when the processing is authorised by EU or Portuguese law providing for appropriate safeguards for the rights and freedoms of individuals. Any comprehensive register of criminal convictions shall be kept only under the control of the official authority.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) requires owners of PI to notify individuals whose data they hold of the following information, among other information, at the time of the PI collection (except where the individuals already hold such information):

- the PI owner's identity and, where applicable (eg, for owners with no permanent establishment in the European Union), that of the owner's representative;
- the contact details of the owner's data protection officer, when appointed;

- the purposes of, and the legal basis for, the PI processing;
- the recipients or categories of recipients of the personal data; and
- other relevant information, including, at least:
  - the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
  - an indication on whether the provision of the PI is a statutory, contractual requirement or a requirement necessary to enter into a contract, as well as whether the individual is required to provide it (and the consequences of failure to provide the PI);
  - the existence (and conditions) for the exercise of the individual's rights to request access from the owner to the PI and rectification or erasure of PI or restriction of processing PI concerning the individual correction thereof or to object to the processing as well as the right to data portability;
  - the existence of automated decision-making using the PI and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such PI processing for the individual;
  - where the processing is based on the consent of the individual, the existence of the right to withdraw consent at any time;
  - the right of the individual to lodge a complaint with a supervisory authority; and
  - an indication on whether the provision of the PI is a statutory, contractual requirement or a requirement necessary to enter into a contract, as well as whether the individual is required to provide it (and the consequences of failure to provide the PI).

Where the PI is not obtained by the PI owner directly from the individual, the provision of the last piece of information is not required but the owner is additionally required to inform the individual on the categories of PI concerned and on the source from which the PI originates, and if applicable, whether it came from publicly accessible sources. In these cases, notification should take place within a reasonable period after the owner obtained the PI, but at the latest within one month or, if earlier, and the PI is to be used for communication with the individual, at the latest at the time the first communication takes place or, if disclosure to third parties is envisaged, at the latest when the PI is first disclosed.

Exemptions from transparency obligations

15 | When is notice not required?

Notice requirement shall not apply:

- where and insofar as the individual already has the information (article 13(4) of the GDPR); or
- where PI has not been obtained from the individual, in any of the following cases:
  - when notice proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in article 89(1) of the GDPR;
  - insofar as notification is likely to render impossible or seriously impair the achievement of the objectives of that PI processing. In such cases the owner shall take appropriate measures to protect the individual's rights and freedoms and legitimate interests, including making notice publicly available;
  - obtaining or disclosure is expressly laid down by EU or Portuguese law and provides appropriate measures to protect the individual's legitimate interests; or
  - where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Portuguese law, including a statutory obligation of secrecy.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

PI processed must be relevant, accurate and, where necessary, kept up to date concerning the purpose for which it is held.

The PI owner is required to take adequate measures to ensure that PI that is inaccurate or incomplete, in light of the processing purpose, is erased or corrected.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The amount of PI that may be held is limited to that which is strictly adequate, relevant and not excessive concerning the purpose for which it is collected and further processed.

The DPA does not specifically allow retention periods, it does, nevertheless, foresee that wherever legal provisions provide for specific retention periods (which, in several cases are set forth as minimum document our information record and retention periods) these will be taken into account by PI owners to set the applicable PI retention periods, the general rule remaining that the PI may not be held for longer than is necessary for the specific purposes for which it was collected and further processed.

There are certain guidelines and decisions issued by the National Commission for the Protection of Data (CNPD) that indicate, for specific purposes, the length of time the authority considers certain categories of PI may be held, which, although issued before the GDPR may also still be considered in the present legal context.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

On PI retention, the DPA does not contain any specific rule fixing the length of time for which PI may be held. The DPA includes a rule stating that the period for which personal data is stored must be the period established by law or regulation or, in the absence of such regulation, the period required in view of the purpose of the processing.

The DPA recognises that where the PI is necessary for the controller or processor to provide evidence of compliance with contractual or other obligations, PI may be retained until the statute of limitation of the corresponding rights is reached.

PI concerning contributions for retirement or pension purposes may be kept without time limitation to assist the pensioner to recover information on his or her career contributions, provided that appropriate technical and organisational measures are taken to safeguard the rights of the data subject.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The finality principle has been adopted in the GDPR and the DPA (the same principle had been previously adopted in local law before the GDPR). Under the GPDR, this is reinforced in light of the principles relating to the processing of personal data provided for in article 5 of the GDPR (eg, the lawfulness, fairness, transparency and the purpose limitation principles). PI may only be collected for specific, express and legitimate purposes and may not be subsequently used for purposes that are incompatible with the same.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The GDPR specifically addresses profiling and automated individual decision-making, including profiling.

Under article 21(1) of the GDPR, the data subject can object to processing (including profiling), on grounds relating to his or her particular situation. Controllers are specifically required to provide for this right in all cases where processing is based on the fact it is necessary for the performance of a task carried out in the public interest, or processing that is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, including profiling based on those provisions. The controller must no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

As a rule, there is a general prohibition on fully automated individual decision-making (ie, with no human involvement in the decision-making process), including profiling, that has a legal or similarly significant effect; although, there are exceptions to the rule. Where one of the exceptions applies, there must be measures in place to safeguard the data subject's rights and freedoms and legitimate interests.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Under article 32 of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), the owner and the service provider are subject to implementing appropriate technical and organisational measures (considering the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of individuals) to ensure a level of security for PI appropriate to the risk. The adequateness of the measures must be assessed considering security and in particular of the risks that are presented by the PI processing, particularly from an accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to PI transmitted, stored or otherwise kept.

Examples of possible measures are also provided by the GDPR under article 32(2), specifically:

- the pseudonymisation and encryption of PI;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to PI promptly in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Law No. 58/2019 of 8 August 2019 (the DPA) provides that the government will identify, through appropriate regulation the minimum security measures and technical requirements that must be adopted by PI controllers and processors when processing health and genetic data, including minimum measures on:

- differentiated PI access permissions, based on a 'need to know' principle and the segregation of roles;
- requirements for prior authentication of access to such PI; and
- a guarantee that logs or other types of electronic registration are kept to allow such data access traceability.

Regulation has been issued indicating minimum security measures and technical requirements – in some cases mandatory; in other cases recommended – as best practices for public entities.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Before the GDPR there was no general obligation to notify the supervisory authority or individuals of data breaches as this was a sector-specific requirement for data breaches in the electronic communications sector, which remains. Under the sector -specific rules, the National Commission for the Protection of Data (CNPD) must be notified of data breaches by the PI owner without undue delay. Also, if the breach was likely to adversely affect individuals (ie, telecom service subscribers or users), PI owners were required to notify the individuals concerned, also without undue delay. In the latter case, a data breach is deemed to affect PI individuals negatively where it may cause identity fraud or theft, physical or reputational damage, or humiliation.

Under the GDPR and the current DPA, the data breach notification obligations to the supervisory authority and communication of a personal data breach to the data subject are provided for under articles 33 and 34 respectively, fully apply. Therefore, a general obligation to notify the supervisory authority (ie, the CNPD) of data breaches has been applicable since 25 May 2018.

Under the current rules, PI breaches must be reported by the PI owner to the CNPD without undue delay and within 72 hours after having become aware of the breach. Only if a PI breach is unlikely to risk harm to the rights and freedoms of the data owners will the reporting requirement be waived. In such cases, the PI owner must still keep a record of the breach and the risk assessment that justified it not reporting the PI breach.

The CNPD has provided PI owners with specific online forms for data breach notification.

When the PI breach is likely to result in a high risk to the rights and freedoms of the affected individuals, the PI owner shall also communicate the breach to the same individuals without undue delay.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Owners of PI are required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law.

Accountability is a principle explicitly laid down among the other structural principles ruling PI processing. Article 5 of the GDPR states that the controller shall be responsible for, and should be able to demonstrate, compliance with all other applicable principles, as laid down in the subparagraphs of paragraph 1 of article 5 of the GDPR.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

In Portugal, before Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), the appointment of a data protection officer was not required. Since 25 May 2018, under the GDPR, certain PI owners (controllers) and processors must appoint a data protection officer (DPO). This is the case for all public authorities and bodies (irrespective of what data they process), and for owners (or processors) that, as a core activity, monitor individuals systematically and on a large scale, or process special categories of personal data on a large scale.

Law No. 58/2019 of 8 August 2019 (the DPA) includes a broad list of entities that qualify as public authority or body to be subject to the duty of designating a DPO.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Before the GDPR, there were no specific or general mandatory requirements for PI owners or processors to maintain internal records or establish internal processes or documentation of the PI processing operations, purposes or activities pursued. The previous system was based on a prior recording of PI processing activities with the supervisory authority, the National Commission for the Protection of Data (CNPD). This has not been the case, ever since the GDPR applied. All PI owners employing 250 or more persons, shall maintain a record of processing activities under their responsibility. Smaller PI owners, nevertheless, shall also keep such record when carrying out PI processing that is likely to result in a risk to the rights and freedoms of individuals, or is not occasional, or includes special categories of PI (sensitive data referred to in article 9(1)) or PI relating to criminal convictions and offences. The same requirement applies to PI processors.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The requirements to carry out a prior assessment of the impact of the envisaged processing operations on the protection of PI under article 35 of the GDPR fully apply in Portugal. The Portuguese supervisory authority has specified the list of PI processing operations likely to result in high risk and that, therefore, require prior data protection impact assessment. The following are among those listed:

- health PI processing with the aid of an implant;
- PI processing involving large-scale profiling;
- biometric PI processing for unique identification of a natural person or processing of genetic PI, involving individuals such as children and employees (vulnerable individuals). except for processing covered by a legal provision that impact has been assessed;
- sensitive PI processing or processing of PI relating to criminal convictions and offences;
- PI of a highly personal nature together with:
  - the use of new or innovative technology;
  - for scientific or historical purpose, public interest archiving purposes or statistical purposes except when authorised by legal provision providing for appropriate safeguards for the fundamental rights and the interests of the individual;
  - based on PI that has not been obtained from the individual and no information may be provided or would involve disproportionate effort to the PI owner; or
- PI processing that involves PI matching or combining;
- processing of location PI or behaviour monitoring PI for evaluation or scoring except if strictly required provide services requested by the individual.

The DPA includes a provision whereby this assessment is not required in the case of PI processing that had been previously authorised by the CNPD, under the previous authorisation (and prior notification) regime.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Under article 25(1) of the GDPR, the PI owner shall, both at the time of the determination of the means for processing the PI and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, effectively and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR and protect the rights of individuals. This must be done considering the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

The PI owner is not required to notify the supervisory authority or obtain prior processing authorisation before any PI processing activities are initiated (except for the prior consultation with the supervisory authority before processing that is required from the PI owner under the terms of article 36 of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), where a data protection impact assessment under article 35 of the GDPR indicates that the processing would result in a high risk in the absence of measures taken by the owner to mitigate the risk).

Law No. 58/2019 of 8 August 2019 (DPA) contains a provision that subjects the use of CCTV systems to prior authorisation from the supervisory authority to be used in surveillance of areas during opening periods, in cases where the system simultaneously captures sound.

Other transparency duties

29 | Are there any other public transparency duties?

There are no general transparency duties in addition to the GDPR requirements.

The DPA includes a general provision requiring that the individual is notified of any access that takes place relating to his or her health data. It is for the PI owner to guarantee that a traceability and notification system is in place.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Entities providing outsourced processing services qualify as processors. The processor must only act on instructions from the PI owner unless he or she is required to act by law.

The PI owner must ensure that the processors it selects provide sufficient guarantees that the required technical and organisational security measures are carried out. Compliance by the processors with the relevant measures must be ensured by the PI owner.

The PI owner and processor must enter into a contract or be mutually bound by an equivalent legal act in writing. The relevant instrument is required to bind the processor to act only on instructions from the owner and must foresee that the relevant security measures are also incumbent on the processor.

All requirements contained in article 28 of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) on the contents of the data processing agreement apply.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Disclosure of PI is generally subject to all the processing principles, restrictions and notification requirements contained in the GDPR and Law No. 58/2019 of 8 August 2019 (DPA). Individuals must be notified at the time of collection or before disclosure takes place for the first time to the categories of entities to which disclosure of PI will be made. Disclosure, as is the case with all other processing acts, must be based on one of the legitimate processing grounds. This may be, in certain cases, the individual's consent.

Health and sex life PI can be disclosed only to health professionals or other professionals also subject to the same secrecy duties.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The transfer of PI to another EU member state or EEA member country is not restricted.

Transfer of PI outside these territories is restricted. In this case, a transfer is permitted only when it is compliant with the DPA requirements and when the state to which PI is transferred ensures an adequate level of protection assessed in the light of all the circumstances surrounding PI transfer, with special consideration being given to the nature of PI to be transferred, the purpose and duration of the proposed processing, the country of final destination, the rules of law in force in the state in question (both general and sector rules) and the professional rules and security measures that are complied with in such country.

PI may flow from Portugal to non-EU or non-EEA member states that have been covered by an adequacy decision issued by the European Commission, acknowledging that such country ensures an adequate level of protection because of its domestic law or of the international commitments it has entered into. A transfer may also be made under contracts that follow the standard form model clauses approved by the European Commission (ie, standard contractual clauses considered to provide appropriate safeguards within the meaning of article 46(1) and (2)(c) of the GDPR by the Commission Implementation Decision (EU) 2021/914 of 4 June 2021). These should be combined with the adoption of measures in line with Recommendations 01/2020 issued by the European Data Protection Board.

Before the GDPR, the Portuguese authority did not accept binding corporate rules for the transfer of PI. This is now admitted under the terms of article 47 of the GDPR.

Following the Court of Justice of the European Union's landmark judgment in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Case C-311/18) of 16 July 2020, in which the Court declared the US–EU Privacy Shield invalid, the EU–US Privacy Shield framework is currently not a valid option for exporting data from the European Union to the United States. The National Commission for the Protection of Data (CNPD) has not guided the impact of the decision. Currently, the standard contractual clauses approved by the European Commission will probably prove to be the most feasible alternative for EU-based entities to continue with the transfer of PI required in the context of their activities, subject, therefore, to appropriate data transfer agreements to be executed. In any case, entities must keep in mind that these agreements will probably need to be modified to reflect updates promised by the European Commission to same-standard clauses, to take full account of GDPR provisions, particularly those outlined in article 28 of the GDPR on data-processing agreements between data controllers and data processors. In the absence of an adequacy decision under article 45(3) of the GDPR or appropriate safeguards under article 46 of the GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the conditions indicated in article 49(a) to (g), if:

- the individual has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for him or her due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the individual and the controller or the implementation of pre-contractual measures taken at the individual's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the PI owner 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 individual or of other persons, where the individual is physically or legally incapable of giving consent; or
- the transfer is made from a register that according to EU or Portuguese law is intended to provide information to the public and that 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 Portuguese law for consultation are fulfilled in the particular case.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions that apply to transfers outside the European Union and European Economic Area between PI owners apply equally in the case of transfers of PI to service providers (processors).

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

The law does not require PI or a copy of PI to be retained in Portugal, notwithstanding that it is transferred or accessed from outside Portugal.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals are granted the right to access their personal information held by PI owners. Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) provides for the right of access, fully applicable in Portugal. Under the right of access, an individual is entitled to obtain confirmation from the owner whether or not PI concerning him or her is being processed, and, where that is the case, access to the PI and relevant information on the processing of it. The right of access also entitles the individual to obtain a copy of the PI undergoing processing from the owner.

When notifying the individuals whose PI they hold, the owners of PI must include information on the existence and conditions for the exercise of the individual's rights of access to PI and correction thereof.

Other rights

36 | Do individuals have other substantive rights?

Individuals are entitled to require the rectification of inaccurate information from the PI owner as well as the update of the information held.

Individuals also have the right to object at any time to the processing of information relating to them:

- on justified grounds; or
- in any case, and free of charge, if the information is meant for direct marketing or any other form of research.

Additionally, individuals are entitled to the right not to be subject to a decision that produces legal effects concerning them or significantly affecting them, which is based solely on automated processing of information intended to evaluate certain personal aspects relating to the same individual.

Correction, removal and information blocking rights are also granted to individuals when the information held by the PI owner does not comply with the provisions set out in the DPA, including cases where the information is incomplete or inaccurate.

All other substantive rights granted to individuals by the GDPR fully apply, such as:

- the erasure of PI or restriction of processing concerning the individual;
- the right to object to processing; and
- the right to PI portability.

Where the processing of the PI is based on the consent of the individual, the individual is granted the right to withdraw the consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

In the event an individual suffers damage as a result of an act or omission purported by the PI owner in breach of the PI protection legislation, the same individual is entitled to compensation for damage claimable through the courts. Compensation for serious injury to feelings may be also claimed.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights to claim monetary damage and compensation are exercisable through the judicial system and not directly enforced by the supervisory authority.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Employee biometric PI may only be used for access control (to premises) and worktime control and recording.

When public contracting formalities require that PI is publicised (eg, official gazette publications or equivalent) no PI other than the name of the individual should be published whenever that is sufficient to guarantee the identification of the public contractor and counterparty.

There is a specific rule restricting the use of CCTV in certain areas (inside or outdoors).

Law No. 58/2019 of 8 August 2019 does not include derogations, exclusions or limitations other than those already described.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Portugal has adopted legislation implementing article 5.3 of Directive 2002/58/EC, as amended by Directive 2009/136/EC (the ePrivacy Directive). The implementation came into effect on 30 August 2012.

Except for essential cookies, such as those that enable core website functionality, the use of cookies requires the individuals' consent (ie, they must opt-in to their use) after having been provided with clear and comprehensive information on the use of cookies, as well as on the categories of PI processed and the purposes thereof.

There has been no explicit provision on the nature of consent, neither has the authority issued formal guidelines on its understanding, but the system implemented in Portugal is understood as being an opt-in solution.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

The use of automated calling and communication systems without human intervention (automatic calling machines), fax machines or email for direct marketing is allowed only in respect of individuals who have given their prior explicit consent. This rule does not apply to users

that are not individuals (legal persons). In this case, unsolicited communications for direct marketing purposes may be sent except where the recipient, being a legal person, expresses its opposition.

Unsolicited communications for direct marketing purposes through email also apply to text, enhanced messaging service, multimedia messaging service and other kinds of similar applications.

These rules do not exclude the possibility of a PI owner, having obtained the electronic contact of its customers in the context of the sale of its products or services, using such contact details for direct marketing of its own products or similar ones. In this case, the PI owner must only provide its customers with the possibility of objecting, free of charge and in an easy manner, to such use. This possibility must be given both at the time of collection of the PI and on the occasion of each marketing message sent to the customer.

All direct marketing messages must identify the PI owner and indicate a valid contact point for the recipient to object to future messages being sent.

All entities sending unsolicited communications for direct marketing purposes must keep an updated list of individuals that have given their consent to receive such communications, as well as a list of customers that have not objected to receiving it.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no special rules explicitly covering targeted online advertising in Portugal, but the provisions on cookies (and equivalent behaviour tracking) for targeted advertising – transposing the ePrivacy Directive – are relevant, and the use of cookies for profiling and targeted advertising purposes requires consent from the relevant data subjects.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Sensitive categories of personal information, currently known, according to the wording of article 9 of the General Data Protection Regulation (GDPR), as 'special categories of data', are subject to more stringent rules. Sensitive categories of data cover the following: genetic, biometric, health, sex life, sexual orientation, political opinion, trade union membership, religious or philosophical belief and racial or ethnic origin data and data on suspicion of illegal activities, criminal or administrative offences and decisions applying criminal penalties, security measures, administrative fines or additional conviction measures.

As a rule, the processing of special categories of PI is prohibited, with exceptions provided for in article 9 of the GPDR. The DPA does not provide for any additional exceptions.

Profiling

44 | Are there any rules regarding individual profiling?

The GDPR specifically addresses profiling and automated individual decision-making, including profiling.

Profiling is defined in article 4(4) of the GDPR as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. The GDPR qualifies as profiling automated processing of PI for evaluating personal aspects, particularly to analyse or make predictions about individuals. Controllers can carry out profiling if they can meet all the principles and have a lawful basis for the processing.

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Helena Tapp Barroso
htb@mlgts.pt

Tiago Félix da Costa
tfcosta@mlgts.pt

Rua Castilho, 165
1070-050 Lisbon
Portugal
Tel: +351 21 381 74 00
Fax: +351 21 381 74 99
www.mlgts.pt

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There are no specific rules of guidance issued by the Portuguese authority on the use of cloud computing. The general DPA rules on PI transfers and the use of processors by PI owners will fully apply in the case of cloud computing services contracted by the owner.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Notwithstanding the protracted negotiation period, the European Parliament and Council Regulation concerning the respect for private life and the protection of personal data in electronic communications (the ePrivacy Regulation) to replace Directive 2002/58/EC (ePrivacy) is at a critical point, after the consolidated version of the ePrivacy Regulation draft proposal was adopted by the Council of the European Union in the first quarter of 2021. The importance of the ePrivacy provisions lies in the fact it is expected to bring a comprehensive system of provisions on PI protection and other end-user privacy protection concerns in electronic communications.

Romania

Alina Popescu, Cristina Crețu, Sonia Benga and Alexandra Mihailov
MPR Partners

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The main legislative framework consists of the following:

- Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), is directly applicable to Romanian legislation;
- Law No. 190/2018 on implementing measures of the GDPR; and
- Law No. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing (DPA).

Guides and recommendations of the European Data Protection Board, as well as guides issued by the DPA, must be considered.

Alongside the above-mentioned legislation, there are a series of normative acts that are relevant from a data protection perspective, including acts that regulate specific areas of data protection, such as cookies and marketing communication.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Romanian data protection authority is the DPA.

The DPA is organised as an independent institution. Its powers are based both on the GDPR and on Law No. 102/2005.

The DPA may conduct investigations, including unannounced ones. During investigations, the DPA may request any documents and information and can access any equipment (including personal data storage equipment) it deems necessary for the purposes of the inspection. The DPA may gather witness statements and commission expert reports.

Once a breach of legislation has been ascertained, the DPA may impose reprimands or fines, alongside corrective measures. Periodic fines can be imposed in specific cases.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Whenever the activity of the controller or processor of personal data has a cross-border nature, a conflict of competence may arise. The mechanism of solving the conflict of competence is enshrined in the GDPR. As a rule, the supervisory authority of the main or single establishment of the controller or processor is competent to act as the lead supervisory authority for investigating the cross-border processing carried out by that controller or processor and must cooperate with the other supervisory authorities concerned.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under Romanian law, the breaches of data protection law are sanctioned by way of:

- reprimands;
- fines; and
- corrective measures in line with the GDPR. Also, the DPA may request the controller and processor to publish at its own cost any of the corrective measures imposed.

An infringement is determined by the control personnel of the DPA and the sanction is applied via a report signed by the same. Where the fine exceeds €300,000, it can be imposed only through a DPA presidential decision, based on the report made by the DPA's control personnel.

Fines are set out in the GDPR from:

- up to €10 million or up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements such as obligations entailed by the privacy by design and privacy by default principle and security of the processing; and
- up to €20 million or up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements related to, for example, the basic principles for processing, including conditions for consent and the data subjects' rights.

If there is non-compliance with the imposed measures, or tacit or express refusal to provide all the information and documents requested by the DPA, or if the controller or processor refuses to be subject of an investigation, the DPA may apply a periodic fine of 3,000 lei per day.

Under the GDPR, Romania decided that a punitive regime should apply to public authorities under the provision of Law No. 190/2018. Therefore, if a public authority infringes the GDPR or the national data protection laws, the DPA issues, in the first phase, a warning accompanied by a remediation plan. The DPA can resume the investigation and if it finds that the measures from the remediation plan were not implemented, a fine ranging from 10,000 to 200,000 lei might be applied.

Romania decided not to impose criminal penalties for infringements.

1.5 Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

The GDPR provides that the decisions issued by DPAs should be accompanied by appropriate safeguards such as effective judicial remedy and due process.

In this respect, national legislation (Law No. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority) provides that the decision of the DPA can be appealed before the competent court. The decision of the court of first instance can be appealed before the competent court of appeal.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The general data protection legal regime enshrined in Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) expressly excludes from its scope of application:

- the processing of personal data performed during activities outside the scope of EU law;
- the processing of personal data performed by EU member states concerning common foreign and security policy;
- the processing of personal data performed by a natural person in the course of a purely personal or household activity;
- the processing of personal data performed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; and
- the processing of personal data of deceased persons.

The legal regime of personal data processing is also regulated by other specific pieces of legislation, that cover the processing of personal data in electronic communications and the processing of personal data while preventing, detecting, investigating, prosecuting and fighting crimes or executing penalties and education and security measures.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Interception of communications, electronic marketing and monitoring and surveillance of individuals are specifically addressed by Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector specifically addresses this subject (that transposes into Romanian legislation Directive 2002/58/EC (the ePrivacy Directive)). Interception of communications and monitoring and surveillance of individuals is further regulated by the Criminal Procedure Code.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Currently, Romania has not developed sector-specific data protection legislation. However, some specific rules (as enabled by the GDPR) are included in the national legislation, regarding the processing of:

- genetic, biometric and health data;
- the national identification number;
- data in employment contexts; and
- data in the context of performing a task that serves a public interest.

These rules do not diverge from the principles and rules of the GDPR.

PI formats

9 | What categories and types of PI are covered by the law?

The GDPR (and thus applicable national legislation) applies to the processing of personal data wholly or partly by automated means and to the processing, other than by automated means, of personal data that forms part of a filing system or is intended to form part of a filing system, where a 'filing system' means any structured set of personal data that is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or a geographical basis.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The GDPR also applies to controllers and processors not established in the European Union when processing activities relate to the offering of goods or services to data subjects in Romania, irrespective of whether a payment from the data subject is required; and monitoring of data subjects' behaviour that takes place in Romania.

Also, the GDPR applies to the processing of personal data by a controller not established in the European Union, but in a place where Romanian law applies under public international law.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

PI is not a concept recognised in EU law. Therefore, the term to be used is 'personal data'. The GDPR applies where the processing of personal data is done wholly or partly by automated means and where the processing other than by automated means of personal data forms part of a filing system or is intended to form part of a filing system. The processing of personal data covers all the operations, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction.

All processing activities that are in the scope of the GDPR must observe the rules set in the same.

The majority of obligations and duties sit with the person who determines the purposes and the means of the processing (the controller), as the controller is accountable for the processing activities of the personal data. Some specific obligations and duties also sit with the person designated by the controller to process data on its behalf (the processor).

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

For any personal data processing activity to be lawful, a legal ground must apply. According to Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), for general categories of data (eg, name, surname, address and bank account), the processing is lawful when:

- the data subject has consented to the processing;
- it is necessary for the performance of a contract to which the data subject is party or is necessary for taking the steps before concluding that contract;
- it is necessary for meeting a legal obligation of the controller;
- it is necessary for protecting the vital interests of the data subject or of another natural person;
- is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; and
- the controller or a third party has a legitimate interest to process the personal data, except for the case when such interests are overridden by the 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.

Regarding special categories of data (eg, health data, genetic and biometric data, data about political opinions and religious and philosophical beliefs), as a rule, any related processing is forbidden. By way of exception, the GDPR expressly provides in what situations the processing may be carried on, as follows:

- the data subject has expressly given his or her consent;
- the data subject has made public the data;
- for employment, social security and social protection when authorised by law;
- for vital interest;
- for reasons of substantial public interest when the law provides;
- for legal claims;
- for health or social care in the public interest when the law provides; and
- for archiving, research and statistics in the public interest when the law provides.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

There are three categories of personal data for which the processing rules differ:

- general personal data;
- special categories of data (eg, race and ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data and health data), that have strict rules for processing; and
- personal data for which the GDPR provides that EU member states can lay out different regimes (ie, personal identification numbers, health data, the processing of personal data in the contexts of employment or fulfilling a task serving the public interest).

If the processing of a personal identification number is based on the legitimate interest of the controller or of a third party, Law No. 190/2018 provides that:

- a data protection officer must be appointed;
- appropriate safeguards must be implemented to observe the minimisation principle and to ensure the security and confidentiality of the processing of data;
- a retention period must be set; and
- periodical training for the persons in charge of processing personal data must be conducted.

In respect of genetic, biometric and data concerning the health of the data subject, Law No. 190/2018 provides that the processing of such data for profiling or automated decision-making process is allowed only when the data subject has given his or her consent in this respect or if specific legal provisions provide so.

For the processing of personal data in the employment context, Law No. 190/2018 provides that for monitoring (based on legitimate interest) employees through electronic communications or video surveillance, the employer must, among other conditions set by the law, consult with the relevant trade union or representatives of the employees and set a retention period that cannot exceed 30 days, save for the situation when the law provides otherwise.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) (and consequently, the Romanian legislation) requires the persons collecting data (controllers) to provide data subjects with specific information at the moment of data collection – if that data is obtained directly from the data subject or within a reasonable period after obtaining the personal data, but at the latest within one month after obtaining the data – when personal data has not been obtained from the data subject (in this latter case, the data subject can also be notified of the processing at the time of the first communication or when the data is first disclosed to a third party; in both cases, the one-month time frame is observed).

The notification must include information on the following:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis of the processing;
- where processing is based on a legitimate interest, the legitimate interests pursued by the controller or by a third party;
- the categories of personal data concerned (when personal data is not obtained from the data subject);
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the intention of the controller to transfer the data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission or, where applicable, the appropriate or suitable safeguards and how to obtain a copy of them or where they have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing or to object to processing, as well as the right to data portability;
- the existence of the right to withdraw consent at any time, when the processing is based on consent;
- the right to lodge a complaint with a supervisory authority;

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
- from which source the personal data originates, and if applicable, whether it came from publicly accessible sources (for when the data is not obtained directly from the data subject, in addition to the information mentioned in all the above points).

Exemptions from transparency obligations

15 | When is notice not required?

When the data is obtained directly from the data subject, there is no need to inform the data subject of the processing if the data subjects already have the information.

When the data is collected from other sources as the data subject, there is no need to inform the data subject when:

- the data subject already has the information;
- informing the data subject is impossible or would require a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to various conditions and safeguards provided by the GDPR or as in so far the obligation to inform is likely to render impossible or seriously impair the achievement of the objectives of that practices. In such cases, the data controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- obtaining or disclosure of the personal data is expressly regulated by specific legislation and the controller provides safeguards for the data subject's legitimate interests; and
- where the personal data must remain confidential subject to an obligation of professional secrecy, including a statutory obligation of secrecy.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

According to the GDPR, the controller must take every reasonable step to ensure that personal data is accurate and up to date (accuracy principle). In this respect, the controller must ensure that the inaccurate personal data, having regard to the purposes for which it is processed, is erased or rectified without delay.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

According to the data minimisation principle set by the GDPR (and, consequently, by national legislation), the collected personal data must be limited to what is necessary concerning the purposes for which it is processed. However, the law does not expressly prescribe rules with regard to restricting types or volumes of personal data that can be collected by controllers.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

According to the storage limitation principle set by the GDPR (and, consequently, by national legislation), the collected personal data must not be kept longer than necessary for the purposes for which such personal data is processed. National legislation, in some cases, provides for data retention periods (eg, for accounting data: 10 years; and for employee payment accounting data: 50 years).

The GDPR does not prescribe specific retention periods for each category of personal data processed or for each processing activity.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The GDPR imposes on controllers the obligation to process personal data only for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes (the 'purpose limitation' principle).

The processing of personal data for purposes other than those for which the personal data was initially collected is allowed where:

- it is based on the data subject's consent;
- it is based on the laws of the European Union or EU member state; or
- where the processing is compatible with the purposes for which the personal data was initially collected.

The GDPR relevant for the finality principle is the 'purpose limitation' principle. According to it, personal data may only be collected for specified (defined), explicit (clear) and legitimate purposes (legal basis) determined at the moment of collection.

The further processing activity is allowed if the personal data is processed for:

- archiving, scientific, historical or statistical purposes as far as appropriate technological and organisational measures are in place to protect the rights and freedoms of the data subjects, in particular, the principle of data minimisation; and
- another purpose compatible with the purpose for which the personal data was initially collected. A compatibility test is required in this case. When assessing the compatibility, the controller should consider:
  - the relationship between the purposes for which the personal data was collected and the further processing purpose;
  - the reasonable expectations of the data subject, as to the further use of his or her personal data; and
  - the nature of the personal data, the possible consequences for data subjects and the existence of appropriate safeguards (such as encryption and pseudonymisation).

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The GDPR provides that a data subject has the right not to be subject to a decision based solely on automated processing if the decision has legal effects on, or other similar effects with significant impact on, the data subject.

However, the above-mentioned right will not be applicable where the automated decision is:

- necessary for concluding or for the performance of a contract between the data subject and the data controller;
- authorised either by the European Union or the law of a member state to which controller is subject and that provides for sufficient safeguards for the rights and freedoms of the data subject; or
- based on the explicit consent of the data subject.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Under the 'integrity and confidentiality' principle, the data controllers are required to process personal data in a manner that ensures appropriate security of the data. This covers protection against unauthorised or unlawful processing and accidental loss, destruction or damage by the implementation of appropriate technical and organisational measures. Both controllers and processors are responsible for the implementation of appropriate technical and organisational measures to process personal data securely. A case-by-case risk assessment is needed.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The data breach notification's regime is regulated by Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and it is applicable across all industries. Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector (Electronic Communications Law) imposes a sector-specific duty to notify personal data breaches, applicable only for the electronic communications service providers.

In both cases, the notification must be submitted to the National Supervisory Authority for Personal Data Processing (DPA), with the mention that under the GDPR the time frame for submission is 72 hours since becoming aware of the incident, while under the Electronic Communications Law the notification must be submitted 24 hours after discovering the incident.

The threshold for notification under the GDPR is a risk-based one. The controller must submit the notification to the DPA when it is likely that the personal data breach will create a risk to the rights and freedoms of natural persons. Also, in what concerns the communication to the data subject, the controller must notify the same about the data breach when it is likely that the data breach will result in a high risk for the data subject.

Based on Electronic Communication Law, all data breaches covered by the law must be notified to the DPA. Also, as a rule, the electronic communications provider must notify the subscriber about the incident when the data breach could affect the personal data or privacy of a subscriber or another person, except for when the electronic communication provider can demonstrate in a manner that the DPA finds satisfying that appropriate measures for the protection of the personal data affected by the incident have been implemented.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The GDPR provides that the data controller is accountable for the observance of the key data protection principles and it should be able to demonstrate the compliance with such principles.

The GDPR requires that the controller embed data protection by design within its organisation. Based on this legal obligation, the controller must implement appropriate technical and organisational measures both at the time it determines the means for processing and at the time it processes the personal data. These technical and organisational measures are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards into the processing activity as to meet GDPR requirements and to protect the data subjects rights.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

As per Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), there are three situations in which the appointment of a data protection officer (DPO) is mandatory, namely:

- when the processing is carried by a public authority or body (including government departments);
- where the core activities of the controller or processor consist of data processing operations that, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale; or
- where the core activities of the controller or the processor consist of the large-scale processing of special categories of data or personal data relating to criminal convictions or offences.

However, the National Supervisory Authority for Protection of Personal Data (DPA) also expressly recommends the appointment of a DPO in those cases when it is not mandatory to appoint such, considering the beneficial role that the DPO may play in ensuring the observance of the GDPR's provisions by the controller or processor. The Article 29 Working Party also recommends that, save for the situation where it is obvious that the designation of a DPO is not mandatory, the internal assessment to determine if a DPO is to be appointed must be documented, in line with the accountability principle.

Under Law No. 190/2018, the appointment of a DPO is mandatory when a controller decides to process personal identification numbers based on legitimate interest.

The DPO's responsibilities are:

- informing and advising the controller, processor or their employees on their duties arising from the data protection legislation;
- monitoring compliance with the GDPR, national data protection legislation and the data protection-related policies of the controller or processor, including carrying out the related audits;
- the assignment of responsibilities, awareness-raising and training of staff tasked with personal data processing;
- providing advice, where requested, regarding the data protection impact assessments and monitoring the performance of the same; and

- cooperation with and acting as the contact point for the DPA.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The GDPR introduced, for both the controllers and processors, the obligation to keep records in writing, including in electronic form, of the processing activities under their responsibilities.

The controller must keep a registry with the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the DPO;
- the purposes of the processing;
- a description of the categories of data subjects and the categories of personal data;
- the categories of recipients to whom personal data has been or will be disclosed;
- transfers of personal data to a third country or an international organisation;
- the envisaged time limits for erasure of the different categories of data; and
- a general description of the technical and organisational security measures in place.

The processor must keep a registry with the following information:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative and the DPO;
- the categories of processing carried out on behalf of each controller;
- transfers of personal data to a third country or an international organisation and safeguards implemented for such transfers; and
- a general description of the technical and organisational security measures in place.

Companies with less than 250 employees are exempted from this obligation, save for the cases when the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or data related to criminal convictions or offences. More information on the derogations is set in the position paper published by the Article 29 Working Party.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

According to the GDPR, where the controller processes personal data using, in particular, new technologies that are based on the nature, scope, context and purposes of the processing, it is likely to result in a high risk to the data subject's rights and freedoms. The controller, prior to starting the processing activity, must carry out a data processing impact assessment (DPIA) concerning the impact the envisaged processing activity will have on the protection of personal data. Based on the examples provided by the GDPR, the DPA issued a decision containing a non-exhaustive list of situations where a DPIA is required (eg, in the case of systematic monitoring on a large scale of a publicly accessible area, such as video surveillance in malls, stadiums, parks, plazas or other similar places).

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Embedding privacy by design and privacy by default are now both legal requirements under the GDPR. Moreover, not ensuring the implementation of the same represents an infringement of the GDPR and is a criterion considered by the DPA when assessing whether to impose an administrative fine. Thus, the controller, regardless of the type of data processed or the nature of the processing, must implement appropriate technical and organisational measures (eg, pseudonymisation, data minimisation and enabling the data subject to monitor the data processing) from the moment of determining the means for processing and at the time of the processing itself. Also, the controller must ensure that only the data that are necessary for each specific purpose of the processing are processed.

The controller also has a duty to carry a data protection impact assessment before a personal data processing activity that is likely to result in a high risk to the rights and freedoms of the data subjects. Such risk could be physical, material or non-material. Building on the cases expressly mentioned by the GDPR, the DPA issued a decision that comprises a list of cases in which the data protection impact assessment is required (eg, in the case of systematic monitoring of a publicly accessible area on a large scale, such as video surveillance in malls, stadiums, parks, plazas or other similar places). The list is non exhaustive.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

In Romania, no obligation of registration with the National Supervisory Authority for Personal Data Processing exists since Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) became applicable on 25 May 2018.

Other transparency duties

29 | Are there any other public transparency duties?

The GDPR imposes on controllers the transparency obligation towards the processing activities and they are obliged to demonstrate compliance with it.

The transparency principle mandates to provide, in writing, or by other means, including, where appropriate, by electronic means, relevant information to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Under Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), the concept of transfer implies that personal data is transmitted from a controller or processor located in the European Economic Area to international organisations, controllers, processors or other recipients located outside it. Otherwise, the transmission of personal data to a provider of processing services located in the European Economic

Area will be regulated by a contract or other binding act, depending on its qualification as a processor, controller or joint controller concerning the processed personal data and does not imply a transfer in the sense of the GDPR.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

There are no specific restrictions regarding the disclosure of personal data to other recipients.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The cross-border transfer of personal data between controllers or processors located in the European Economic Area is permitted without restriction. However, for cross-border transfers outside the European Union and European Economic Area (either to a third country or to an international organisation), as a rule, the transfer of personal data is not allowed, save for the following situations:

- based on an adequacy decision issued by the European Commission, provided that the third country has implemented safeguards that ensure the protection of personal data and the rights and freedoms of the data subjects; and
- based on appropriate safeguards implemented by the controller or processor who transfers the personal data.

Some examples of appropriate safeguards include binding corporate rules, standard data protection clauses adopted by the European Commission or adopted by a supervisory authority and approved by the European Commission. In cases where the appropriate safeguards are provided through simple contractual clauses, an authorisation from the competent National Supervisory Authority for Protection of Personal Data (DPA) is mandatory.

However, following the invalidation of the EU–US Privacy Shield by the Court of Justice of the European Union's decision in *Schrems II*, transfers of personal data to third countries pose some problems owing to the potential extraterritorial effect of surveillance laws in those third countries. In such cases, the transfer tools mentioned above might not be sufficient when used as legal basis for the transfer.

The European Data Protection Board's Recommendations on supplementary measures to be used to ensure that the transferred data benefits from the same level of protection as the one ensured in the European Union.

The data exporters now must perform a transfer impact assessment (TIA) to properly evaluate that the transfer tool intended to be used is effective against the legislation and practices of the third country. Depending on the TIA result, the data exporter will need to further investigate the need for implementing supplementary technical, contractual and organisational measures to either go on with, suspend or stop the transfer.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes, the restrictions are applicable for any type of transfer, as regulated by the GDPR, irrespective of the quality of the recipient. As for onward transfers, the same conditions under which the first transfer was made must be also applied for the onward transfer, so that the same level of protection is ensured.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

The GDPR provides that the free movement of personal data within the European Union cannot be restricted nor prohibited for reasons connected with the protection of natural persons with regard to processing of personal data.

Currently, there are no national provisions in place requiring personal data or a copy thereof to be retained within the Romanian jurisdiction.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

The data subject has the right to confirmation on whether the controller processes his or her data and to access that information.

The data subject is entitled, upon specific request, to a copy of the personal data that is processed. Further copies can be subject to a reasonable fee by the controller. That right shall not adversely affect the rights and freedoms of others.

The controller must also provide a list of details that replicates the information that must be provided under the transparency obligation (article 13 and 14 of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR)).

Other rights

36 | Do individuals have other substantive rights?

Other substantive rights of the data subject, apart from the access right, are:

- the right to information (ie, the right to be informed of the processing);
- the right to rectification (ie, the right to rectify any inaccuracies in the processed data);
- the right to be forgotten (ie, the right to the erasure of the processed data, in certain conditions);
- the right to a restriction (ie, the right to obtain the restriction of the processing of data, in certain conditions);
- the right to data portability (ie, the right to receive from the controller the personal data concerning the data subject in a structured and machine-readable format to transmit those data to another controller, subject processing activities have as a legal base a contract with or the consent of the data subject and they are carried out by automated means);
- the right of objection (ie, the right to oppose the processing, in certain conditions);
- the right not to be subjected to automated decision-making (ie, the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or adversely affects the data subject); and
- the right to lodge a complaint with a supervisory authority.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The GDPR provides for an effective judicial remedy, as well as for compensation, whenever the rights of data subjects have been breached.

In Romania, monetary compensation is available for both material and moral damages. However, the award of monetary compensation for moral damages is to be granted by a court of law following a substantiated request to this end submitted by the affected data subject.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights of the data subjects can be enforced by the National Supervisory Authority for Personal Data Processing or directly through effective judicial remedies when the data subjects consider that their rights have been breached.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

In Romania, the law implementing Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) provides for derogations for processing of data for journalistic purposes or the purpose of academic, artistic or literary expression, as well as for scientific or historical research purposes, artistic or public archiving purposes.

Processing for journalistic purposes or the purpose of academic, artistic or literary expression may be carried out if it concerns personal data that has been manifestly made public by the data subject or that is closely linked to the data subject's capacity as a public person or the public nature of the facts in which it is involved, without the applicability of specific chapters from the GDPR, such as, among other things, the chapters regarding the principles, the rights of the data subjects and others.

Certain rights of the data subject provided by the GDPR will not apply where the rights make it impossible or seriously affect the achievement of the specific objectives and such derogations are necessary for the fulfilment of those purposes. This includes personal data being processed for:

- scientific or historical research purposes, for statistical purposes, namely:
  - the right of access;
  - the right to rectification;
  - the right to restrict processing; and
  - the right to object; or
- archiving purposes in the public interest, namely:
  - the right to be informed;
  - the right of access;
  - the right to rectification;
  - the right to erasure;
  - the right to restrict processing;
  - the right to data portability; and
  - the right to object.

The derogations mentioned above apply only where the processing is subject to appropriate safeguards under the GDPR.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector (the Electronic Communications Law), transposed Directive 2002/58/EC (the ePrivacy Directive) into Romanian legislation regulates the use of cookies. Related to cookies, the Electronic Communications Law provides two cumulative conditions for storing information or gaining access to information stored in the terminal equipment of a subscriber or user when:

- the subscriber or user has given his or her consent; and
- before giving consent, the subscriber or user was provided with clear, complete and easy to understand information related to the purposes of the processing.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

The regime for marketing by electronic communications means is regulated by the Electronic Communications Law that transposed the ePrivacy Directive into Romanian legislation. Sending marketing communications using automated means that do not require human intervention, such as through fax, email or any other method that uses electronic communication services aimed at the public is not permitted if the user or the subscriber has not expressly given his or her prior consent. As an exception, where a natural or legal person obtains, in the context of the sale of a product or a service, the email address of its customers, the same natural or legal person may use the email address for direct marketing of its own similar products or services provided that customers are clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such receiving at the time of their collection and on the occasion of each message, if the customer has not initially refused such use.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules regarding targeted online advertising. Processing personal data for the purpose of targeted online advertising must observe the rules enshrined in the GDPR.

Where tracking technologies are used in connection with targeted online advertising, the provisions of Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector (transposing into the national legislation the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector) are also applicable.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The GDPR provides in article 9 the conditions under which the special categories of personal data are processed.

As a general rule, processing of special categories of personal data (namely, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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.

By way of exception, the GDPR expressly provides those situations where the processing of special categories of personal data is permitted, as follows:

- the data subject has expressly given his or her consent;
- the data is manifestly made public by the data subject;
- for employment, social security and social protection when authorised by law;
- for vital interest;
- for reasons of substantial public interest when law provides;
- for legal claims;
- for health or social care in the public interest when law provides; and
- for archiving, research and statistics in the public interest when law provides.

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific requirements regarding profiling. Depending on the type of profiling and its degree of intrusiveness, either the general rules prescribed by the GDPR or the provisions of article 22 of the GDPR on automated individual decision-making, including profiling, will be applicable.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The cloud computing service is defined under Law No. 362/2018 concerning measures for a high common level of security of network and information systems that transposes Directive (EU) 2016/1148 into national legislation. However, Romanian law does not provide specific rules applicable to cloud computing services.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Currently, there are no emerging trends or hot topic regarding data protection.

Alina Popescu
alina.popescu@mprpartners.uk

Cristina Crețu
cristina.cretu@mprpartners.com

Sonia Benga
sonia.benga@mprpartners.com

Alexandra Mihailov
alexandra.mihailov@mprpartners.com

6A Barbu Delavrancea Street
Building C, Ground Floor
1st District
Bucharest 011355
Romania
Tel +40 21 310 1717
www.mprpartners.com
www.mprpartners.uk

Singapore

Lim Chong Kin
Drew & Napier LLC

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The main data protection legislation in Singapore is the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA).

The PDPA applies to all organisations that collect, use or disclose personal data in Singapore unless one of the exclusions under section 4 of the PDPA applies. The main data protection obligations imposed on organisations concerning the collection, use, disclosure, access to, correction and care of personal data are set out in Parts III to VIB of the PDPA (the Data Protection Provisions).

The PDPA also provides for the establishment of the Personal Data Protection Commission (PDPC), the data protection authority.

The PDPA recently underwent its first comprehensive review since its enactment in 2012. The Personal Data Protection (Amendment) Act 2020 (the Amendment Act), which was passed in Parliament on 2 November 2020, sets out extensive changes, the majority of which came into effect on 1 February 2021.

There are various regulations and advisory guidelines under the PDPA that deal with specific issues in greater detail. For example, the Personal Data Protection Regulations 2021 (the PDP Regulations) supplement the PDPA in four key areas:

- the requirements for transfers of personal data out of Singapore;
- the assessment relating to the processing of personal data in reliance of the grounds of deemed consent by notification and legitimate interests;
- the form, manner and procedures for making and responding to requests for access to or correction of personal data; and
- persons who may exercise rights concerning disclosure of personal data of deceased individuals.

The other regulations issued under the PDPA include:

- the Personal Data Protection (Composition of Offences) Regulations 2021;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2021;
- the Personal Data Protection (Appeal) Regulations 2021; and
- the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

Also, the PDPC has issued several advisory guidelines and guides to provide greater clarity on the interpretation of the PDPA. The PDPC has also developed sector-specific advisory guidelines for:

- the telecommunications sector;
- the real estate agency sector;
- the education sector;
- the healthcare sector;
- the social services sector;
- transport services for hire (specifically concerning in-vehicle recordings); and
- for management corporations.

On 20 February 2018, Singapore became the sixth Asia-Pacific Economic Cooperation (APEC) economy to participate in the APEC Cross-Border Privacy Rules (CBPR) system. Singapore also became the second APEC economy to participate in the APEC Privacy Recognition for Processors (PRP) system. Collectively, the CBPR and PRP systems allow a smoother exchange of personal data among certified organisations in participating economies and ensure that data protection standards are maintained for consumers in the Asia-Pacific region.

The formulation of the PDPA framework has taken into account international best practices on data protection. As indicated during the second reading of the PDPA in Parliament, the then Minister of Information, Communications and the Arts had referred to the data protection frameworks in key jurisdictions such as Canada, New Zealand, Hong Kong and the European Union, as well as the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework, in developing the PDPA framework.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The PDPA is administered and enforced by the PDPC. With effect from 1 October 2016, the PDPC has been subsumed as a department under the Info-communications Media Development Authority (IMDA).

The PDPC may initiate an investigation to determine whether an organisation complies with the PDPA, upon receipt of a complaint or on its own motion.

According to the Advisory Guidelines on Enforcement of Data Protection Provisions, the factors that the PDPC may consider in deciding whether to commence an investigation include:

- whether the organisation may have failed to comply, whether intentionally, negligently, or for any other reason or cause, with all or a significant part of its obligations under the PDPA;
- whether the organisation's conduct indicates a systemic failure by the organisation to comply with the PDPA or to establish and

maintain the necessary policies and procedures to ensure its compliance;
- the number of individuals who are, or may be, affected by the organisation's conduct;
- the impact of the organisation's conduct on the complainant or any individual who may be affected;
- whether the organisation had previously contravened the PDPA or may have failed to implement the necessary corrective measures to prevent the recurrence of a previous contravention; and
- public interest considerations.

In the course of its investigation, the PDPC's powers include:
- requiring any organisation to produce any specified document or to provide any specified information;
- compelling the attendance of witnesses, the provision of information and the production of documents;
- entering an organisation's premises without a warrant (by giving at least two working days' advance notice of intended entry); and
- obtaining a search warrant to enter an organisation's premises and search the premises or any person on the premises (the latter, if there are reasonable grounds for believing that he or she has in his or her possession any document, equipment or article relevant to the investigation), and take possession of, or remove, any document and equipment or article relevant to an investigation.

The PDPC is also empowered to review complaints concerning access, correction and data porting requests.

The PDPA also establishes the Data Protection Advisory Committee, which advises the PDPC on matters relating to the review and administration of the personal data protection framework, such as key policy and enforcement issues.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The PDPC may enter into a cooperation agreement with a foreign data protection authority for data protection matters such as cross-border cooperation. Cooperation may take the form of information exchange or any other assistance as necessary to assist in the enforcement or administration of data protection laws.

Specifically, section 10 of the PDPA provides that the cooperation agreement has to be entered into for the purposes of:
- facilitating cooperation between the PDPC and another foreign data protection authority in the performance of their respective functions insofar as those functions relate to data protection; and
- avoiding duplication of activities by the PDPC and another foreign data protection authority, being activities involving the enforcement of data protection laws.

In this regard, the cooperation agreement may include provisions to:
- enable the PDPC and the other foreign data protection authority to furnish to each other information in their respective possession if the information is required by the other for the purpose of performance by it of any of its functions;
- provide such other assistance to each other as will facilitate the performance by the other of any of its functions; and
- enable the PDPC and the other foreign data protection authority to forbear to perform any of their respective functions concerning a matter in circumstances where it is satisfied that the other is performing functions concerning that matter.

Under the PDPA, the PDPC may only furnish information to a foreign data protection authority pursuant to a cooperation agreement if it requires of and obtains from that authority an undertaking in writing by it that it will comply with terms specified in that agreement, including terms that correspond to the provisions of any written law concerning the disclosure of that information by the PDPC.

Where the information requested contains personal data that is treated as confidential under the PDPA, the PDPC may only disclose the information to the foreign data protection authority if the following conditions are specified:
- the information or documents requested by the foreign data protection authority are in the possession of the PDPC;
- unless the government otherwise allows, the foreign data protection authority undertakes to keep the information confidential at all times; and
- the disclosure of the information is not likely to be contrary to the public interest.

The PDPC is also a participant in the Asia Pacific Economic Corporation Cross-border Privacy Enforcement Arrangement (APEC CPEA), which creates a framework for the voluntary sharing of information and provision of assistance for privacy enforcement-related activities.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Generally, the powers of the PDPC in the enforcement of any breach of data protection law include:
- powers relating to alternative dispute resolution (ADR);
- powers relating to review applications; and
- powers of investigation.

Any individual affected by an organisation's non-compliance with any of the Data Protection Provisions may lodge a complaint with the PDPC. Upon receipt of a complaint, the PDPC may investigate or review the matter, or direct the parties as to the appropriate mode of dispute resolution.

Concerning ADR, under section 48G(1) of the PDPA, the PDPC is provided with the power to establish or approve one or more dispute resolution schemes, and direct complainants to resolve disputes via mediation, without the need to secure the consent of both parties.

As to the type of enforcement action it may take, the PDPC may choose to do any one of the following:
- suspend or discontinue an investigation;
- initiate an undertaking process;
- issue an expedited breach decision;
- initiate a full investigation; or
- impose criminal penalties.

Suspend or discontinue an investigation

The PDPC may discontinue investigations and simply issue an advisory notice where the impact is assessed to be low. Section 50 of the PDPA sets out circumstances in which the PDPC may do so, including where a complainant has not complied with a direction, the parties involved have mutually agreed to settle, or any party has commenced legal proceedings in respect of any contravention of the PDPA.

Voluntary undertaking

The PDPC may accept a voluntary undertaking from any organisation, which includes a written agreement between the organisation and the PDPC in which the organisation voluntarily commits to remedy the

breaches and take steps to prevent a recurrence. The organisation's request to invoke the undertaking process must be made very soon after the incident is known. The PDPC is unlikely to accept an undertaking request in certain cases (eg, where the organisation refutes responsibility for the data breach incident, or where it is a repeat incident entailing a similar cause of the breach).

Section 48L of the PDPA empowers the PDPC to accept statutory undertakings from an organisation when the PDPC has reasonable grounds to believe that an organisation has not complied, is not complying or is likely not to comply with the PDPA.

Where an organisation is found not to have complied with any term of the voluntary undertaking, the PDPC may take action that it thinks fit in the circumstances, which may include issuing directions and imposing available enforcement remedies.

Expedited breach decision

The PDPC may issue an expedited breach decision at its discretion in certain circumstances where there is an upfront, voluntary admission of liability for breaching relevant obligations under the PDPA. The expedited breach decision will achieve the same enforcement outcome as a full investigation. Where financial penalties are involved, the organisation's admission of its role in the incident could be taken as a mitigating factor. However, admissions are unlikely to be considered as a strong mitigating factor for repeated data breaches. The organisation must make a written request to the PDPC for an expedited decision very soon after the incident is known to the organisation.

Full investigation process

For incidents with high impact, and where facilitation or mediation is inappropriate in the circumstances (eg, where there is a disclosure of personal data on a large scale or where the personal data disclosed could cause significant harm), the PDPC may initiate a full investigation.

Where the PDPC is satisfied that an organisation has intentionally or negligently contravened any of the Data Protection Provisions under the PDPA, it is empowered with wide discretion to issue such remedial directions as it thinks fit. These include directions requiring the organisation to:

- stop collecting, using or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA;
- provide access to, correct or port personal data, or reduce or make a refund of any fee charged for any access, porting or correction request; or
- pay a financial penalty of up to S$1 million.

Concerning the quantum of financial penalty, the Amendment Act will empower the PDPC to impose higher financial penalties (ie, up to a maximum of 10 per cent of the organisation's annual turnover in Singapore, or S$1 million, whichever is higher). However, this provision will only come into effect from 1 October 2022.

In assessing the seriousness of a data breach, the PDPC may consider several factors, including the following:

- impact of the organisation's breach;
- whether the organisation actively took reasonable steps to resolve the matter effectively and promptly;
- whether the organisation had known or ought to have known the risk of a serious contravention and failed to minimise the risk;
- whether the organisation obstructed the PDPC during investigations;
- whether the organisation failed to comply with a warning or direction from PDPC;
- whether the organisation, which handles a large volume of sensitive personal data, failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such data;
- whether the organisation took immediate steps to notify affected individuals of the breach and reduce the damage caused by a breach; and
- whether the organisation voluntarily notified the PDPC of the breach as soon as it learned of the breach and cooperated with the PDPC in its investigations.

To date, the PDPC has issued more than 100 published grounds of decisions, with a significant majority of these cases relating to breaches of the Protection Obligation (ie, section 24 of the PDPA). On 15 January 2019, the PDPC imposed its highest financial penalties to date of S$250,000 and S$750,000 respectively on SingHealth Services Pte Ltd (SingHealth) and Integrated Health Information Systems Pte Ltd, for breaching their data protection obligations under the PDPA. This unprecedented data breach, which arose from a cyberattack on SingHealth's patient database system, caused the personal data of some 1.5 million patients to be compromised.

Any person who suffers loss or damage directly as a result of a contravention of any of the Data Protection Provisions may also commence a private civil action in respect of such loss or damage suffered.

Criminal penalties

Part IXB of the PDPA sets out offences relating to the egregious mishandling, by individuals, of personal data in the possession of or under the control of an organisation or a public agency:

- under section 48D, if an individual discloses, or causes the disclosure of, personal data in the possession or control of an organisation or a public agency to another person, which is not authorised, and the individual does so knowingly, or is reckless to the disclosure not being authorised, the individual shall be guilty of an offence; and
- under section 48E, if an individual makes use of personal data in the possession or control of an organisation or a public agency which is not authorised, the individual does so knowingly, or is reckless to the use not being authorised, and as a result of the use of the personal data, the individual:
  - obtains a gain;
  - causes harm to another individual; or
  - causes loss to another person, that individual shall be guilty of an offence.

Under section 48F, if an individual takes any action to reidentify or cause reidentification of anonymised information in possession or control of an organisation or a public agency, which is not authorised, and the individual does so knowingly, or is reckless to the re-identification not being authorised, that individual shall be guilty of an offence.

The penalty for these offences is a fine not exceeding S$5,000 or imprisonment for a term not exceeding two years, or both. However, certain defences are provided for in respect of these offences, for example, where the accused used, disclosed or reidentified the data in the reasonable belief that the accused had the legal right to do so, and was not reckless as to whether this was so.

Section 51 of the PDPA also sets out certain offences relating to, among others, obstructing or hindering the PDPC in the performance of any function or duty, or the exercise of any power, under the PDPA. It is also an offence for an organisation or a person, without reasonable excuse, to neglect or refuse to either provide any information or produce any document that the organisation or person is required to provide or produce to the PDPC or an inspector or attend before the PDPC or inspector as required.

1.5 Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

With respect to avenues of appeal under the PDPA, organisations and individuals aggrieved by enforcement decisions or directions of the PDPC may, within a specified time period, either apply to the PDPC for reconsideration or appeal to the chair of the Data Protection Appeal Panel as per the Personal Data Protection (Appeal) Regulations 2021.

Appeals against, or with respect to, a direction or decision of a Data Protection Appeal Committee may be made to the General Division of the High Court on a point of law or as to the amount of a financial penalty (section 48R(1) of the PDPA). The High Court shall hear and determine the appeal, and may: confirm, modify or reverse the direction or decision of the Appeal Committee; and make a further or other order on such appeal, whether as to costs or otherwise, as the High Court may see fit (section 48R(3) of the PDPA). A decision of the High Court under section 48R(3) of the PDPA may be further appealed to the Court of Appeal in accordance with the Rules of Court.

As a public authority, any administrative action by the PDPC may also be subject to judicial review by the courts, provided that the relevant thresholds and conditions are met (eg, exhausted other possible alternative remedies).

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA) applies to all organisations in Singapore, regardless of their scale or size.

An 'organisation' is defined broadly under the PDPA as including any individual, company, association or body of persons, corporate or unincorporated, and whether or not formed or recognised under the law of Singapore, or resident or having an office or place of business in Singapore.

Certain categories of organisations are carved out of the application of the Data Protection Provisions of the PDPA, such as:

- individuals acting in a personal or domestic capacity;
- employees acting in the course of their employment with an organisation (although employees may be liable for the egregious mishandling of personal data in the possession of or under the control of an organisation or a public agency); and
- public agencies.

The PDPA is intended to set a baseline standard for personal data protection across the private sector, and will operate alongside (and not override) existing laws and regulations. The PDPA provides that the general data protection framework does not affect any right or obligation under the law and that in the event of any inconsistency, the provisions of other written laws will prevail.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

To the extent that personal data is collected, used or disclosed in the interception of communications and in the monitoring and surveillance of individuals, the PDPA applies to the organisation collecting, using or disclosing such data. As such, the individual's prior consent is required before any collection takes place unless an exception to consent applies or the collection is otherwise authorised under law.

Also, where an organisation collecting such personal data via the interception of communications or the performance of surveillance or monitoring activities is a public agency (eg, the Singapore Police Force or the Info-communications Media Development Authority (IMDA)), such collection is excluded from the application of the PDPA.

Apart from the PDPA, there are provisions in other laws or regulations that allow for the interception of communications and the monitoring and surveillance of individuals. Below is a non-exhaustive list of such provisions:

- Organisations providing telecommunications services and holding services-based operations licences may have to comply with interception requests by the IMDA and other authorities. Specifically, condition 16.2 of the IMDA's standard Services-Based Operator (Individual) (SBO (I)) licence conditions expressly permit disclosure of subscriber information where the disclosure of subscriber information is deemed necessary to the IMDA or such other relevant law enforcement or security agencies in the exercise of their functions or duties. Condition 26.1 of the IMDA's standard SBO (I) licence conditions also requires licensees to 'provide the [IMDA] with any document and information within its knowledge, custody or control, which the [IMDA] may, by notice or direction require'.
- Section 20 of the Criminal Procedure Code (Cap 68) empowers the police to require the production of a 'document or other thing' (which is necessary or desirable for any investigation, inquiry, trial or another proceeding under the Code) by issuing a written order to 'the person in whose possession or power the document or thing is believed to be'.
- Section 10 of the Kidnapping Act (Cap 151) states that the Public Prosecutor may authorise any police officer to, amongst others, 'intercept any message transmitted or received by telecommunication' or 'intercept or listen to any conversation by telephone'.
- Section 19 of the Cybersecurity Act 2018 (No. 9 of 2018) (the Cybersecurity Act) states that where information regarding a cybersecurity threat or incident has been received by the Commissioner, he or she may exercise certain powers as are necessary to investigate the cybersecurity threat or incident, including the power to require the provision of any document in a person's possession or information considered to be related to the matter.

Electronic marketing

Generally, where the personal data of an individual is collected, used and disclosed for marketing purposes, the consent of the individual concerned must be obtained and such consent must not have been obtained as a condition for the provision of a product or service where it would not be reasonably required to provide that product or service. The Personal Data Protection Commission (PDPC) has noted in its Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised 1 February 2021) (Key Concepts Guidelines) that a failure to opt out will not be regarded as consent in all situations, and recommended that organisations obtain consent from an individual through a positive action of the individual (eg, opt-in consent).

Concerning the sending of marketing communications by telephone call or text messaging (or fax) to a Singapore telephone number, Part IX of the PDPA (ie, the Do Not Call (DNC) Provisions) requires an organisation to:

- obtain valid confirmation that the telephone number is not listed on the relevant DNC Register before sending the message or call unless clear and unambiguous consent to the sending of the specified message to that number is obtained in evidential form;
- be identified as a marketing message, and include information identifying the sender for messages and details on how the sender

can be readily contacted, and such details and contact information should be reasonably likely to be valid for at least 30 days after the sending of the message; and
- for voice calls, not conceal or withhold the calling line identity from the recipient.

A limited exception exists concerning sending messages to individuals with whom the organisation has an ongoing relationship.

Concerning the duty to check the DNC Registry, section 43A of the PDPA imposes obligations on third-party checkers to communicate accurate DNC Register query results to the organisations that they are checking the DNC Register on behalf of.

Further, Part IXA of the PDPA contains a prohibition concerning the sending of applicable messages to telephone numbers generated or obtained through the use of dictionary attacks and address harvesting software.

The DNC Provisions (which used to be enforced as criminal offences) are now enforced under the same administrative regime as the Data Protection Provisions. If the organisation is found to have intentionally or negligently contravened any provision, the PDPC may require the organisation to pay a financial penalty not exceeding:
- S$200,000, in the case of an individual; or
- S$1 million, in any other case.

For a contravention of the prohibition on the use of dictionary attacks and address-harvesting software under the DNC Provisions, the maximum financial penalty will increase to 5 per cent of the organisation's annual turnover in Singapore, where the organisation's annual turnover in Singapore exceeds S$20 million. However, this enhanced financial penalty will only come into effect on 1 October 2022.

Complementing the DNC Provisions of the PDPA, the Spam Control Act (Cap 311A) (the Spam Control Act) regulates the bulk sending of unsolicited commercial electronic messages to email addresses or mobile telephone numbers.

Section 11 read with the Second Schedule of the Spam Control Act requires any person who 'sends, causes to be sent or authorises the sending of unsolicited commercial electronic messages (which includes emails, instant messages (on platforms such as Telegram and WeChat) and short message service or multimedia message service) in bulk' to comply with certain obligations. These include, among others, requirements that unsolicited commercial electronic messages must contain:
- an unsubscribe facility;
- the label '<ADV>' to indicate that the message is an advertisement; and
- the message must not contain header information that is false or misleading.

Section 9 of the Spam Control Act also prohibits electronic messages from being sent to electronic addresses generated or obtained through the use of a dictionary attack or address-harvesting software.

The Spam Control Act provides for civil liability (including the grant of an injunction or the award of damages) against parties in breach of these requirements. Statutory damages of up to S$25 per message may be awarded, up to an aggregate of S$1 million (unless the plaintiff proves that his or her actual loss is higher).

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Before the enactment of the PDPA, Singapore did not have an overarching law governing the protection of PI, or personal data. The collection, use, disclosure and care of personal data in Singapore were regulated to a certain extent by a patchwork of laws including common law, sector-specific legislation and various self-regulatory or co-regulatory codes. These existing sector-specific data protection frameworks continue to operate alongside the PDPA.

Various other laws and regulations in Singapore set out specific data protection rules, some of which are sector-specific. For instance:
- the Banking Act (Cap 19) prescribes the disclosure of customer information by a bank or its officers;
- the Computer Misuse Act (Cap 50A) deals with computer system hackers and other similar forms of unauthorised access or modification to computer systems;
- the Cybersecurity Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore to ensure that computers, systems and data are better protected;
- the Private Hospitals and Medical Clinics Act (Cap 248) contains provisions relating to the confidentiality of information held by private hospitals, medical clinics, clinical laboratories and healthcare establishments licensed under the Act;
- the Official Secrets Act (Cap 213) contains provisions relating to the prevention of disclosure of official documents and information;
- the Public Sector (Governance) Act 2018 (No. 5 of 2018) sets out directions for data sharing among government agencies and imposes criminal penalties on public officers who recklessly or intentionally disclose data without authorisation, misuse data for a gain or re-identify anonymised data; and
- the Telecom Competition Code issued under the Telecommunications Act (Cap 323) contains certain provisions pertaining to the safeguarding of end-user service information.

Concerning the financial sector, the Monetary Authority of Singapore (MAS) is empowered under the Monetary Authority of Singapore Act (Cap 186) and other sectoral legislation to issue directives and notices. Examples of MAS-issued regulatory instruments which are relevant to data protection include the Notices on Cyber Hygiene, Notices and Guidelines on Technology Risk Management, Notices and Guidelines on Prevention of Money Laundering and Countering the Financing of Terrorism, and the Guidelines on Outsourcing. These regulations operate alongside the PDPA and prevail to the extent of any inconsistency.

PI formats

9 | What categories and types of PI are covered by the law?

All formats of PI are covered under the PDPA, whether electronic or non-electronic and regardless of the degree of sensitivity. 'Personal data' is broadly defined under the PDPA as data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

Nonetheless, the PDPA provides for certain exceptions and limitations for the applicability of the Data Protection Provisions for certain types of personal data, such as personal data that is contained in a record that has been in existence for at least 100 years, or 'business contact information' as defined under the PDPA.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Data Protection Provisions apply to all organisations that collect, use or disclose personal data in Singapore, regardless of whether they are formed or recognised under Singapore law or whether they are resident or have an office or place of business in Singapore. As such,

organisations that are located overseas are still subject to the Data Protection Provisions as long as they collect, use or disclose personal data in Singapore. Also, organisations that collect personal data overseas and host or process it in Singapore will be subject to the relevant obligations under the PDPA from the point that such data is brought into Singapore.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Yes, the PDPA regulates the collection, use and disclosure of personal data by an organisation. An organisation that collects, uses or discloses personal data is accordingly required to comply with the Data Protection Provisions under the PDPA.

A 'data intermediary', however, is exempt from the majority of the Data Protection Provisions under the PDPA. A data intermediary refers to an organisation that processes personal data on behalf of and for the purposes of another organisation (the primary organisation) pursuant to a written contract.

A data intermediary is only required to comply with the rules relating to:

- the protection of personal data (section 24);
- the retention of personal data (section 25); and
- the duty to notify the primary organisation without undue delay where it has reason to believe that a data breach has occurred concerning personal data that it is processing on the primary organisation's behalf (sections 26C(3)(a) and 26E).

A data intermediary that processes personal data in a manner that goes beyond the processing required under the written contract would not be considered a data intermediary and is subject to the full suite of Data Protection Provisions under the PDPA in respect of that processing.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes, the processing of personal data includes 'collection, use and disclosure' of the same under the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA). An individual's consent is required before an organisation can collect, use or disclose such individual's personal data unless otherwise required or authorised by law. Such consent must be validly obtained and may be either expressly given or deemed to have been given.

For consent to be considered validly given, the organisation must first inform the individual of the purposes for which his or her personal data will be collected, used or disclosed. These purposes have to be what a reasonable person would consider appropriate in the circumstances.

Consent obtained via the following ways does not constitute valid consent for the purpose of the PDPA:

- where consent is obtained as a condition of providing a product or service, and such consent is beyond what is reasonable to provide the product or service to the individual; and
- where false or misleading information is provided, or deceptive or misleading practices are used, to obtain or attempt to obtain the individual's consent for collecting, using or disclosing personal data.

The PDPA stipulates that consent is deemed to have been given in certain circumstances, specifically:

- Deemed consent by conduct: where an individual voluntarily provides his or her personal data to the organisation for a particular purpose, and it is reasonable that the individual would voluntarily provide his or her personal data.
- Deemed consent by contractual necessity: where the disclosure of personal data from organisation A to organisation B is necessary for the conclusion or performance of a contract or transaction between the individual and organisation A. This deemed consent by contractual necessity also extends to disclosure by B to another downstream organisation C where the disclosure by B (and collection by C) is reasonably necessary to fulfil the contract between the individual and A.
- Deemed consent by notification: subject to the organisation's fulfilment of preconditions such as the conduct of an assessment to determine that the proposed processing of personal data is not likely to have an adverse effect, an individual may be deemed to have consented to the organisation's collection, use or disclosure of his or her personal data for a purpose that he or she has been notified of. In this deemed consent by notification, the organisation must provide a reasonable period for the individual to opt-out before it proceeds to collect, use or disclose the personal data. Consent for the collection, use or disclosure of personal data is deemed to be given only after the opt-out period has lapsed.

While consent is generally required, the First and Second Schedules to the PDPA provide for specific situations where personal data can be collected, used or disclosed without the individual's consent. Such exceptions to consent include those relating to:

- vital interests of individuals;
- public interests;
- legitimate interests;
- business asset transactions;
- business improvement purposes; and
- research.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

The PDPA does not expressly distinguish between the types and sensitivities of personal data. However, as a number of the Data Protection Provisions adopt a standard of reasonableness, the sensitivity of the personal data in question could, in practice, affect the regulatory outcome concerning a contravention of the relevant provision.

For instance, section 24 of the PDPA requires that an organisation would need to make 'reasonable security arrangements' to protect personal data in its possession or under its control, to prevent:

- unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
- the loss of any storage medium or device on which personal data is stored.

The Personal Data Protection Commission (PDPC) has noted that organisations should take into account the sensitivity of personal data when deciding on the appropriate level of security arrangements needed to protect it.

Notably, the PDPC imposes more stringent guidelines concerning National Registration Identity Card (NRIC) numbers and other national identification numbers. According to the Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (issued on 31 August 2018), organisations are generally not allowed to collect, use

or disclose NRIC numbers and other national identification numbers unless such collection, use or disclosure is required under the law (or an exception under the PDPA applies), or is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The obligation to notify individuals stems primarily from the process of seeking valid consent for the processing of personal data. In particular, organisations are obliged to inform individuals of:

1 the purposes for the collection, use or disclosure of his or her personal data, on or before collecting the personal data;
2 any other purpose for the use or disclosure of personal data that has not been notified to the individual under (1), before such use or disclosure of personal data; and
3 on request by the individual, the business contact information of a person who can answer the individual's questions about the collection, use or disclosure of the personal data on behalf of the organisation.

Only after the above information has been notified to the individual can he or she be considered to have validly given his or her consent to the collection, use or disclosure of his or her personal data under the purposes made known to him or her.

While the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA) requires that such notice be provided to the individual on or before the collection, use and disclosure of his or her personal data, there is no prescribed manner or form in which such a notice must be given.

More generally, the PDPA requires that an organisation makes information available about its data protection policies and practices. This would typically be satisfied through an external data protection notice.

Exemptions from transparency obligations

15 | When is notice not required?

The First and Second Schedules to the PDPA set out respectively certain circumstances where an individual's consent need not be obtained for the collection, use and disclosure of his or her personal data. Accordingly, the requirement to notify the individual would generally not apply under such circumstances.

However, section 20(4) of the PDPA is an exception to the rule. An organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of or concerning the organisation:

- entering into an employment relationship with the individual or appointing him to any office; or
- managing or terminating an employment relationship with, or appointment of, the individual, must notify the individual of that purpose (despite the fact there is no requirement to seek consent).

Moreover, under section 20(5) of the PDPA, the organisation is also required to, upon request, provide the business contact information of a person who can answer questions about such processing of personal data.

Similarly, where an organisation intends to collect, use or disclose personal data by relying on the exception for 'legitimate interest' purposes, the PDPA requires the organisation to disclose its reliance.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes, section 23 of the PDPA generally requires that organisations make a reasonable effort to ensure that the personal data they collect is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual or is likely to be disclosed by the organisation to another organisation. This is regardless of whether the personal data is collected directly by the organisation or on behalf of the organisation.

The Personal Data Protection Commission (PDPC), in its Key Concepts Guidelines, has stated that an organisation must make a reasonable effort to ensure that:

- it accurately records the personal data it collects (whether directly from the individual concerned or through another organisation);
- the personal data it collects includes all relevant parts thereof (so that it is complete);
- it has taken the appropriate (reasonable) steps in the circumstances to ensure the accuracy and correctness of the personal data; and
- it has considered whether it is necessary to update the information.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The PDPA does not specifically restrict the types or volume of PI that may be collected. However, section 18 of the PDPA provides that organisations may collect, use or disclose personal data only for purposes that a reasonable person would consider appropriate.

Further, the PDPC clarified in its Advisory Guidelines on the PDPA for the National Registration Identity Card (NRIC) and other National Identification Numbers (issued on 31 August 2018), that to comply with section 18 of the PDPA, organisations generally must not collect, use or disclose NRIC numbers and other national identification numbers unless such collection, use or disclosure is required under the law (or pursuant to an exception under the PDPA), or is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Yes, section 25 of the PDPA provides that organisations (including data intermediaries) should cease to retain personal data, or remove how it can be associated with particular individuals, as soon as it is reasonable to assume that such retention no longer serves the purposes for which the data was collected, and retention is no longer necessary for legal or business purposes. Such legal or business purposes may, for example, include situations where the personal data is required for an ongoing legal action involving the organisation, where retention of the personal data is necessary to comply with the organisation's obligations under other applicable laws, or where the personal data is required for an organisation to carry out its business operations, such as to generate annual reports or performance forecasts.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes, the purposes for which personal data can be used or disclosed by organisations are restricted to the purposes for which the individual

concerned has been informed of and given his or her consent (if applicable). Further, an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.

Generally, fresh consent would need to be obtained where organisations are seeking to collect, use or disclose personal data for different purposes from those to which the individual concerned had given his or her consent, unless there is an applicable exception.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The PDPA does not specifically restrict the use of PI for making automated decisions, including profiling. However, the PDPA's general data protection obligations would apply insofar as there is any collection, use or disclosure of personal data for such purpose (such as the obligation to obtain consent and to use personal data only for purposes that a reasonable person would consider appropriate).

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Section 24 of the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA) requires that organisations protect the personal data in their possession or control by making 'reasonable security arrangements' to prevent:

- unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
- the loss of any storage medium or device on which personal data is stored.

Organisations that process personal data on behalf of an organisation (ie, data intermediaries) are also subject to the same requirement.

While the Personal Data Protection Commission (PDPC) recognises that there is no one-size-fits-all solution in respect of the type of security arrangements, it has, in its Key Concepts Guidelines, advised an organisation to:

- design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;
- identify reliable and well-trained personnel responsible for ensuring information security;
- implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- be prepared and able to respond to information security breaches promptly and effectively.

The PDPC's Guide to Securing Personal Data in Electronic Medium sets out good practices concerning information and communications technology (ICT) security measures that organisations should adopt to protect electronic personal data (eg, concerning ICT security audits and tests, authentication and authorisation, computer networks and email security), while the PDPC's Guide on Managing and Notifying Data Breaches provides guidance for organisations as to the effective preparation for and management of data breaches.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Yes, the relevant provisions may be found in Part VIA of the PDPA. Under section 26A of the PDPA, a 'data breach', concerning personal data, is defined as:

- the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or
- the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

Under section 26B of the PDPA, a data breach is a 'notifiable data breach' if it:

- results in, or is likely to result in, significant harm to any individual to whom any personal data affected by a data breach relates; or
- is, or is likely to be, of a significant scale (ie, 500 or more individuals).

A data breach is deemed to result in significant harm to an individual if it affects any prescribed class of personal data under the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

In the event of a data breach that affects personal data in an organisation's possession or under its control, the organisation is required to conduct an assessment of the data breach to determine if it is a notifiable data breach. If so, the notifiable data breach must be informed to the PDPC, as well as to affected individuals to whom significant harm may result, unless an exception applies.

Obligation to notify the PDPC

Depending on the exact circumstances, organisations may be required to notify the PDPC in the event of a data breach. Section 26D(1) of the PDPA (read with section 26B of the PDPA) requires organisations to notify PDPC of a data breach that is notifiable.

Where an organisation has reason to believe that a data breach has occurred, it must conduct, reasonably and expeditiously, an assessment as to whether the data breach is notifiable. Data intermediaries must notify the organisation for which it is processing personal data on behalf without undue delay. Organisations must notify the PDPC as soon as practicable, but, in any case, no later than three calendar days after determining that the data breach meets the notification criteria (ie, that the data breach is a notifiable data breach).

Obligation to notify affected individuals

Under section 26D(2) of the PDPA, organisations must notify affected individuals if the data breach is likely to result in significant harm or impact to the individuals to whom the information relates. There are two exceptions to this, which are set out under section 26D(5) of the PDPA.

Specifically, these exceptions are:

- where organisations have taken actions under any prescribed requirements that renders it unlikely that the breach will result in significant harm to affected individuals; and
- where the personal data that was compromised by the data breach is subject to technological protection (eg, encryption) such that the data breach is unlikely to result in significant harm to the affected individuals.

Organisations must also not notify affected individuals if instructed by a prescribed law enforcement agency or directed as such by PDPC (eg, in

circumstances where such notification may compromise investigations or prejudice enforcement efforts).

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Part 3 of the Personal Data Protection Act 2012 (PDPA) sets out the general rules with respect to the protection of and accountability for personal data. These general rules include the following:

- an organisation must develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA; and
- an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Yes, it is mandatory to appoint a data protection officer (DPO). Pursuant to the Accountability Obligation under the PDPA, organisations are required to designate one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA (section 11(3) of the PDPA).

This appointed individual (typically known as the DPO) has to have the appropriate expertise and knowledge to be able to ensure that the organisation complies with the PDPA and develops a process to receive and respond to complaints concerning how the organisation applies the PDPA.

The Personal Data Protection Commission (PDPC) recommends that responsibilities of a DPO may include, but are not limited to, the following:

- ensuring compliance of the PDPA when developing and implementing policies and processes for handling personal data;
- fostering a data protection culture among employees and communicating personal data protection policies and processes to stakeholders;
- managing personal data protection-related queries and complaints;
- alerting the management to any risks that might arise concerning personal data; and
- liaising with the PDPC on data protection matters, if necessary.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Section 12 of the PDPA requires an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA and make information about its policies and procedures available on request.

According to the Key Concept Guidelines, organisations should develop both internal and external data protection policies and practices, taking into account the types and amount of personal data it collects and the purposes for such collection.

Risk assessment

26 Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The PDPA expressly requires an organisation to carry out a risk assessment where the organisation intends to collect, use or disclose personal data by relying on either of the following grounds.

Deemed consent by notification

In brief, under section 15A(4)(a) of the PDPA, an organisation may deem that an individual has given consent for a purpose when the individual is notified of the collection, use or disclosure of his or her personal data and how he or she may opt out, but he or she does not opt out within a specified period.

If an organisation intends to rely on this ground, it must conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual.

Legitimate interest

In brief, an organisation can collect, use or disclose personal data without consent about an individual if it is in the legitimate interests of the organisation or another person.

If an organisation intends to rely on this ground, it must conduct an assessment to determine that the legitimate interests of the organisation or other person outweigh any adverse effect on the individual.

In carrying out the risk assessment, an organisation must:

- identify any adverse effects that the proposed collection, use or disclosure of the personal data for the purpose concerned is likely to have on the individual; and
- identify and implement reasonable measures to:
  - eliminate the adverse effect;
  - reduce the likelihood that the adverse effect will occur; or
  - mitigate the adverse effect.

Design of PI processing systems

27 Are there any obligations in relation to how PI processing systems must be designed?

There are no express obligations in the PDPA on how PI processing systems must be designed, such as requiring privacy by design.

However, the Personal Data Protection Commission issued a Guide to data protection practices for ICT systems.

REGISTRATION AND NOTIFICATION

Registration

28 Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no requirement under the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA) for organisations that collect, use or disclose personal data (whether in the capacity of a principal organisation or a data intermediary) to register with the Personal Data Protection Commission (PDPC). However, a data protection officer (DPO) may choose to register with the PDPC to keep abreast of developments in the PDPA.

Other transparency duties

29 | Are there any other public transparency duties?

While there is no express requirement for an organisation to make public statements on the nature of its processing of personal data per se, organisations are required under the Accountability Obligation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, and to make such policies and practices available on request (section 12 of the PDPA).

As part of the Accountability Obligation, an organisation is also required to appoint a DPO and make available his or her business contact information to the public. The DPO must have appropriate expertise and knowledge to be able to ensure that the organisation complies with the PDPA, and must develop a process to receive and respond to complaints concerning how the organisation applies the PDPA.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Organisations that process personal data on behalf of another organisation (the primary organisation) are considered 'data intermediaries' under the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA). Such data intermediaries are exempt from most of the main Data Protection Provisions under the PDPA if they process personal data on behalf of and for the purposes of the primary organisation pursuant to a contract that is evidenced or made in writing.

Data intermediaries are subject only to the Data Protection Provisions relating to the protection and retention of personal data, and the duty to notify the primary organisation without undue delay where it has reason to believe that a data breach has occurred concerning personal data that it is processing on the primary organisation's behalf.

To the extent that these data intermediaries reside overseas or the processing of personal data by such data intermediaries involves the transfer of personal data out of Singapore, the primary organisation would need to comply with the Transfer Limitation Obligation under the PDPA.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

An organisation's disclosure of an individual's personal data to other recipients must be made following the applicable requirements under the PDPA. In other words, if an organisation wishes to disclose an individual's personal data to a third-party recipient, the organisation must first obtain valid consent from the individual himself, which includes providing notification of the specified purposes for which the organisation intends to disclose the individual's personal data, and such purposes are only for purposes that a reasonable person would consider appropriate in the circumstances, unless an exception applies.

Further, in responding to an access request made under section 21 of the PDPA, organisations are not allowed to provide an individual with his or her personal data or other information in certain prescribed circumstances.

Where the disclosure is to a third-party recipient that is outside of Singapore, the organisation must also ensure that it complies with the applicable cross-border data transfer requirements.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Yes, section 26 of the PDPA prohibits organisations from transferring personal data out of Singapore except where such transfer of personal data is following the requirements prescribed under the PDPA, to ensure that organisations provide a standard of protection to the transferred personal data that is comparable to the protection under the PDPA.

Under the Personal Data Protection Regulations 2021 (the PDP Regulations), all organisations transferring personal data from Singapore to countries or territories outside of Singapore are required to ensure that the recipient of such personal data is bound by 'legally enforceable obligations' to provide to the transferred personal data a standard of protection that is at least comparable to the protection accorded under the PDPA. These 'legally binding obligations' include obligations imposed under law, contract, binding corporate rules (for transfers to 'related' organisations), or any other legally binding instrument.

Data transfer agreement

Where the transfer of personal data is pursuant to a contract, contractual clauses are to be contained in a legally binding contract that is enforceable against every receiving organisation under the contract. Such a contract must require the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA and specify the countries and territories to which the personal data may be transferred under the contract.

Binding corporate rules

Where binding corporate rules are used, these rules must:

- require every related recipient of the transferred personal data to provide a standard of protection for the personal data transferred that is at least comparable to the protection under the PDPA;
- specify:
  - the recipients of the transferred personal data to which the binding corporate rules apply;
  - the countries and territories to which the personal data may be transferred under the binding corporate rules; and
  - the rights and obligations provided by the binding corporate rules; and
- only be used for recipients that are related to the transferring organisation.

Notwithstanding, a transferring organisation is taken to have satisfied its obligation to ensure that the recipient is bound by legally enforceable obligations to provide to the transferred personal data a PDPA-comparable standard of protection, in certain circumstances, including where:

- the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party that is entered into at the individual's request;
- the personal data is data in transit (ie, personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed, used by or disclosed to any organisation while the personal data is in Singapore, except for the purpose of such transportation); or
- the personal data is publicly available in Singapore.

Organisations with prescribed certifications

Additionally, under the PDP Regulations, organisations that hold 'specified certifications' that are granted or recognised under the law of the country or territory that the personal data is transferred to, will be taken to be bound by such legally enforceable obligations.

The 'specified certifications' refer to certifications under the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems. An overseas recipient of personal data is taken to be bound by legally enforceable obligations if it:

- is receiving the personal data as an organisation and holds a valid APEC CBPR certification; or
- is receiving the personal data as a data intermediary and it holds either a valid APEC PRP or APEC CBPR certification (or both).

Further transfer

33 If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Where the recipient is a data intermediary, the transferring organisation has to set out minimal protections concerning the protection and retention limitation of the personal data. Where the recipient is an organisation other than a data intermediary, the transferring organisation has to set out protections for the transferred personal data concerning:

- the purpose of collection, use and disclosure of the data by the recipient;
- accuracy of the data;
- security of the data;
- retention period of the data;
- policies on personal data protection; and
- access and correction requests.

Further, the Key Concept Guidelines provides that where an organisation engages a data intermediary to process personal data on its behalf and for its purposes, the organisation continues to be responsible for complying with all Data Protection Obligations under the PDPA as if the personal data were processed by the organisation itself, including the Transfer Limitation Obligation in respect of any overseas transfer of personal data. This is regardless of whether the personal data is transferred by the organisation to an overseas data intermediary, or by a local data intermediary as part of its processing for and on the organisation's behalf. Thus, the onus is on the transferring organisation to undertake appropriate due diligence and obtain assurances when engaging a data intermediary, to ensure that the data intermediary will comply with the requirements under the PDPA, by, for example, having in place appropriate data protection policies and practices (including assurances of compliance with relevant industry standards or certification).

For onward transfers of personal data, the PDP Regulations provide an exemption for 'data in transit', which, in summary, refers to personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed or used by, or disclosed to, any organisation while the personal data is in Singapore, except for the purpose of such transportation. An overseas organisation transferring personal data through Singapore to an overseas destination will be deemed to comply with the Transfer Limitation Obligation in respect of such data in transit.

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no express requirement under the PDPA that requires PI or a copy of PI to be retained in the jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction.

RIGHTS OF INDIVIDUALS

Access

35 Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, under section 21 of the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA), individuals have the right to request an organisation to provide them with their personal data that is in the possession or under the control of the organisation, and information about how that personal data has been or may have been used or disclosed within a year before the date of the access request.

This individual's right of access is not an unfettered one. There are several exceptions as set out in section 21(3) of the PDPA. Organisations are not allowed to provide an individual with his or her personal data or other information where such provision could reasonably be expected to:

1 threaten the safety or physical or mental health of an individual other than the individual who made the request;
2 cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
3 reveal personal data about another individual;
4 reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his or her identity; or
5 be contrary to the national interest.

Concerning exceptions (3) and (4), these two exceptions would not apply to any user activity data about, or any user-provided data from the requesting individual, despite such data containing third-party personal data.

Further, the Fifth Schedule to the PDPA sets out certain situations where organisations are not required to accede to such requests, for example, concerning:

- opinion data kept solely for an evaluative purpose;
- documents relating to a prosecution, if all proceedings related to the prosecution have not been completed;
- personal data that is subject to legal privilege;
- personal data that, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;
- personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed; or
- any request:
  - that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
  - if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;
  - for information that does not exist or cannot be found;
  - for trivial information; or
  - that is otherwise frivolous or vexatious.

Under the Personal Data Protection Regulations 2021 (the PDP Regulations), organisations are entitled to charge the individual a reasonable fee for access to his or her personal data, provided that the organisation gives the individual a written estimate of the fee. This is to allow organisations to recover the incremental costs incurred in the form of time and effort spent by the organisation in responding to the access request. If an individual is not satisfied with the fee that is being charged by the organisation, the individual may, under section 48H(1)(d) of the PDPA, make an application to the PDPC for the PDPC to review the fee, and the PDPC may, upon completion of its review, confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant or receiving organisation (as the case may be).

In terms of response time frame, organisations are required to respond to an access request as soon as reasonably possible. Subject to this, the PDP Regulations provide that, if an organisation is unable to respond to an access request within 30 days from the request, it must inform the individual in writing within that same time frame of the time by which it will be able to respond to the request (which should be the soonest possible time it can provide access).

If an organisation does not accede to an individual's request to provide that individual access to his or her personal data, the individual may make an application to the PDPC to review the organisation's refusal to provide access to personal data requested by the individual, or a failure to provide such access within a reasonable time. Upon completion of its review, the PDPC may confirm the refusal to provide access to the personal data or direct the organisation to provide access to the personal data, within such time as the PDPC may specify.

Additionally, organisations must also preserve a copy of the personal data requested pursuant to an access request for a prescribed period after the rejection of the request or until the individual has exhausted the right to apply for a reconsideration or appeal, whichever is later.

Other rights

36 | Do individuals have other substantive rights?

Correction Obligation

Yes, section 22 of the PDPA provides an individual with the right to request an organisation to correct any error or omission in his or her personal data that is in the possession of or under the control of the organisation. This is, however, subject to certain exemptions (eg, if the request relates to opinion data kept solely by the organisation for an evaluative purpose). Notably, the PDPA also excludes 'derived personal data' from the application of the Correction Obligation. 'Derived personal data':

- means personal data about an individual that is derived by an organisation in the course of business from other personal data, about the individual or another individual, in the possession or under the control of the organisation; and
- does not include personal data derived by the organisation using any prescribed means or method.

Organisations are required to correct the personal data as soon as reasonably practicable. Subject to this, the PDP Regulations provide that, if an organisation is unable to make the necessary correction within 30 days from the request, it is required to inform the individual in writing within the same time frame of the time by which it will be able to do so (which should be the soonest practicable time it can correct).

Unless it is satisfied on reasonable grounds that a correction should not be made, an organisation is required to correct the personal data, and send the corrected personal data to every organisation to which the personal data was disclosed within one year of the date the amendment was made, insofar as that organisation needs the corrected personal data for any legal or business purpose.

Unlike access requests, organisations are not entitled to charge a fee for correction requests.

Withdrawal of consent

An individual may, at any time, withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation (section 16 of the PDPA). Organisations must not prohibit an individual from withdrawing consent and should not have inflexible consent withdrawal policies.

Several requirements must be complied with by either the individual or the organisation concerning a withdrawal of consent:

- the individual must give reasonable notice of the withdrawal to the organisation;
- on receipt of the notice, the organisation must inform the individual of the consequences of withdrawing consent;
- an organisation must not prohibit an individual from withdrawing consent, although this does not affect any legal consequences arising from such withdrawal; and
- upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law.

Data Portability Obligation

Under the Personal Data Protection (Amendment) Act 2020 (the Amendment Act), a new Data Portability Obligation will be introduced. While the provisions relating to data portability (ie, Part VIB of the PDPA) have been passed, the provisions will only come into effect at a later date, together with the issuance of regulations. It is anticipated that these regulations will prescribe further details such as:

- a whitelist of data categories to which the obligation applies;
- the technical and process details for the transmission; and
- safeguards for individuals (eg, cooling-off periods or an establishment of a blacklist of individuals that organisations may refuse to port data to).

When the Data Portability Obligation comes into force, an organisation must, upon receiving a data porting request from an individual, transmit the applicable data about the individual specified in the data porting request to the receiving organisation in a commonly used machine-readable format. The following conditions must be satisfied:

- the data porting request satisfies any prescribed requirements; and
- the porting organisation, at the time it receives the data porting request, has an ongoing relationship with the individual.

A porting organisation is not required to transmit any applicable data about an individual that is:

- specified as excluded applicable data in Part 1 of the Twelfth Schedule; or
- in any of the excluded circumstances specified in Part 2 of the Twelfth Schedule.

The exceptions to the Data Portability Obligation under Part 1 of the Twelfth Schedule mirror those under the Access Obligation. For instance, the Data Portability Obligation will not apply to derived personal data and data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation.

Additionally, a porting organisation must not transmit any applicable data about an individual if:

- the transmission of the applicable data can reasonably be expected to:

- threaten the safety, or physical or mental health, of an individual other than the individual to whom the applicable data relates;
- cause immediate or grave harm to the safety, or physical or mental health, of the individual to whom the applicable data relates; or
- be contrary to the national interest;

- the receiving organisation to which the applicable data is to be transmitted is, or belongs to a class of organisations that is, prescribed to be an excluded receiving organisation; or
- the PDPC directs the porting organisation not to transmit the applicable data.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes, under section 480 of the PDPA, any person who suffers loss or damage directly as a result of non-compliance by an organisation with the Data Protection Provisions under Parts IV to VIB of the PDPA will have a right of action for relief in civil proceedings in a court.

However, where the PDPC has decided the PDPA in respect of such contravention, this right is only exercisable after such a decision issued by the PDPC becomes final after all avenues of appeal have been exhausted. The court may grant relief as it thinks fit, including an award of an injunction or declaration, or damages.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

An individual's right to commence a private action for loss or damage suffered directly as a result of an organisation's non-compliance with the PDPA would be an action for relief in civil proceedings. Such a right is only exercisable provided that any relevant infringement decision issued by the PDPC has become final after all avenues of appeal have been exhausted.

Therefore, if an individual becomes aware that an organisation has failed to comply with the PDPA, such individual may lodge a complaint to the organisation directly, or bring a complaint to the PDPC. Upon receipt of a complaint, the PDPC may then investigate or review the matter, or direct the parties as to the appropriate mode of dispute resolution.

Where the PDPC is satisfied that an organisation has breached the Data Protection Provisions under the PDPA, the PDPC is empowered with wide discretion to issue such remedial directions as it thinks fit, including the imposition of a financial penalty that does not exceed S$1 million. When the amendments under the Amendment Act relating to the quantum of financial penalties come into force from 1 October 2022, this limit will be raised to S$1 million, or 10 per cent of the organisation's annual gross turnover in Singapore, whichever is higher.

Should any organisation or individual be aggrieved by the PDPC's decision or direction, such organisation or individual may request the PDPC to reconsider its decision or direction. Thereafter, any organisation or individual aggrieved by the PDPC's reconsideration decision may submit an appeal to the Data Protection Appeal Panel. Alternatively, an aggrieved organisation or individual may appeal directly to the Data Protection Appeal Panel without first submitting a reconsideration request.

An appeal can be made against the Data Protection Appeal Panel's decision to the High Court on limited grounds, namely on a point of law or where such decision relates to the amount of a financial penalty.

Reconsideration applications and appeal requests must be made within 28 days after the issuance of the relevant direction or decision; there is no automatic suspension of the direction or decision concerned except in the case of the imposition of a financial penalty or the amount thereof.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

Business contact information

The application of the Data Protection Provisions does not extend to 'business contact information', (unless expressly referred to), which is defined as 'an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and other similar information about the individual, not provided by the individual solely for his or her personal purposes'.

Exclusions from DNC Provisions

Concerning the Do Not Call (DNC) Provisions, certain messages are excluded from the meaning of a specified message under the Eighth Schedule to the Personal Data Protection Act 2012 (No. 26 of 2012) and therefore not subject to the application of the DNC Provisions. Such exceptions include the following:

- any message sent by a public agency under, or to promote, any programme carried out by any public agency that is not for a commercial purpose;
- any message sent by an individual acting in a personal or domestic capacity;
- any message that is necessary to respond to an emergency that threatens the life, health or safety of any individual;
- any message the sole purpose of which is:
  - to facilitate, complete or confirm a transaction that the recipient has previously agreed to enter into with the sender;
  - to provide warranty information, product recall information or safety or security information concerning a product or service purchased or used by the recipient; or
  - to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender;
- any message (other than a message set out in the point directly above):
  - that is sent while the sender is in an ongoing relationship with the recipient of the message; and
  - the sole purpose of which relates to the subject matter of the ongoing relationship. An 'ongoing relationship' means a relationship, on an ongoing basis, between the sender and the recipient of the message, arising from the carrying on or conduct of a business or an activity (commercial or otherwise) by the sender;
- any message the sole purpose of which is to conduct market research or market survey; and
- any message sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The Personal Data Protection Commission (PDPC) has noted that any personal data collected through the use of 'cookies' would not be treated differently from other types of personal data, and organisations that collect personal data using cookies would equally be subject to the requirements of the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA). Organisations are only required to obtain consent for cookies that collect personal data. Organisations do not need to obtain consent for cookies that do not collect personal data (eg, session cookies may only collect and store technical data needed to play back a video on a website).

The Selected Topics Guidelines clarify that there may not be a need to seek consent for the use of cookies to collect, use or disclose personal data where the individual is aware of the purposes for such collection, use or disclosure and voluntarily provides his or her personal data for such purposes. Such activities include transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase.

Further, for activities that cannot take place without cookies that collect, use or disclose personal data, consent may be deemed to have been given if the individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he or she would do so.

In situations where the individual configures his or her browser to accept certain cookies but rejects others, he or she may be deemed to have consented to the collection, use and disclosure of the personal data by the cookies that he or she has chosen to accept. However, the mere failure of an individual to actively manage his or her browser settings does not imply that he or she has consented to the collection, use and disclosure of personal data by all websites for their stated purpose.

Also, the Selected Topics Guidelines make clear that where organisations use cookies for behavioural targeting that involves the collection and use of an individual's personal data, the individual's consent is required.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

Organisations that make telemarketing calls or send messages of a commercial nature (which are considered to be 'specified messages' under the Do Not Call (DNC) Provisions) are required to obtain valid confirmation that the Singapore telephone number is not listed in the DNC registry within 21 days before sending the specified message.

This may be done by:

- making an application to confirm whether the Singapore telephone number is listed in the DNC registry; or
- obtaining from checker information that the Singapore telephone number is not listed in the DNC registry.

Organisations may also wish to refer to the PDPC's Advisory Guidelines on Requiring Consent for Marketing Purposes.

Regarding the rules on marketing emails, the Spam Control Act governs the sending of unsolicited electronic communications in bulk in Singapore.

In general, under the Spam Control Act, any person who sends, causes to be sent, or authorises the sending of unsolicited commercial electronic messages in bulk, is required to contain within the message:

- an unsubscribe facility for the recipient to unsubscribe from such messages;
- where there is a subject field, a title in the subject field and that title is not false or misleading as to the content of the message;
- the letters '<ADV>' with a space before the title in the subject field, or if there is no subject field, in the words first appearing in the message, to clearly identify that the message is an advertisement;
- header information that is not false or misleading; and
- an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules relating to targeted online advertising under the PDPA. However, the PDPA's general data protection obligations would apply if there is any collection, use or disclosure of personal data for such purpose (such as the obligation to obtain consent, unless an exception applies under the PDPA).

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The PDPA does not have specific rules relating to the processing of 'sensitive' categories of personal information. However, as a number of the Data Protection Provisions adopt a standard of reasonableness, the sensitivity of the personal data in question could, in practice, affect the regulatory outcome concerning a contravention of the relevant provision.

For instance, section 24 of the PDPA requires that an organisation make 'reasonable security arrangements' to protect personal data in its possession or under its control, to prevent:

- unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
- the loss of any storage medium or device on which personal data is stored.

The PDPC has noted that organisations should take into account the sensitivity of personal data when deciding on the appropriate level of security arrangements needed to protect it.

Notably, the PDPC imposes more stringent guidelines concerning National Registration Identity Card (NRIC) numbers and other national identification numbers. According to the Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (issued on 31 August 2018), organisations are generally not allowed to collect, use or disclose NRIC numbers and other national identification numbers unless such collection, use or disclosure is required under the law (or an exception under the PDPA applies), or is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity.

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific rules relating to profiling under the PDPA. However, the PDPA's data protection obligations would apply if there is any collection, use or disclosure of personal data for such purpose (such as the obligation to obtain consent, unless an exception applies under the PDPA).

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The PDPC's Guide to Securing Personal Data in Electronic Medium provides guidance for organisations that use cloud computing service providers (CCSPs). For instance, organisations that adopt cloud services for the management of personal data need to be aware of the security and compliance challenges that are unique to cloud services, and where the CCSP is unable to customise a service for the organisation, the organisation must decide if the security measures put in place by the CCSP provides reasonable security for the personal data.

CCSPs are required to comply with the PDPA (in particular, the obligation to implement reasonable security arrangements to protect personal data in their possession or under their control), any applicable subsidiary legislation that may be enacted from time to time, and any applicable sector-specific data protection frameworks to the extent that CCSPs provide cloud services to customers operating in these sectors.

Notably, CCSPs are required to make reasonable security arrangements to protect personal data in their possession or under their control. The Selected Topics Guidelines state that industry standards such as the ISO 27001 and Tier 3 of the Multi-Tiered Cloud Security Certification Scheme could assure the CCSP's ability to comply with the Protection Obligation. Additionally, PDPC has stated in its Selected Topics Guidelines that when engaging CCSPs, organisations should ensure that any overseas transfer of personal data will be done following the requirements under the PDPA, namely, that the organisation should ensure that the CCSP uses only transfers data to locations with comparable data protection regimes, or has legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data. This is regardless of whether the CCSP is located in Singapore or overseas. The organisation may be considered to have taken appropriate measures to comply with the Transfer Limitation Obligation by ensuring that personal data may only be transferred to overseas locations with comparable data protection laws, or that the recipients (eg, data centres or sub-processors) in these locations are legally bound by similar contractual standards.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA) has been amended by the Personal Data Protection (Amendment) Act 2020 (the Amendment Act). The Personal Data Protection (Amendment) Bill 2020 was introduced in the Singapore Parliament on 5 October 2020 and passed by the Singapore Parliament on 2 November 2020 as the Amendment Act. Most of the changes introduced by the Amendment Act came into effect on 1 February 2021, including the introduction of a new Data Breach Notification Obligation, and changes to the consent framework.

The increased cap for financial penalties will come into effect on 1 October 2022.

The new Data Portability Obligation will come into effect at a later date.

Lim Chong Kin
chongkin.lim@drewnapier.com

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315
Tel +65 6535 0733
www.drewnapier.com

South Korea

Kwang Hyun Ryoo, Juho Yoon, Tae Uk Kang, Minwoon Yang and Minyoung Kim

Bae, Kim & Lee LLC

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

In Korea, the collection and use of PI is mainly governed by the Personal Information Protection Act (PIPA), together with the ensuing regulations and guidelines. PIPA resembles the EU General Data Protection Regulation (GDPR) in scope and thrust, but differs in key aspects, including the main legal basis for PI collection (express informed consent, not legitimate interests) and requisites for PI transfers (more extensive than under the GDPR). Korea obtained an EU adequacy decision under the GDPR in December 2021.

Other statutes, with their related guidelines, become relevant depending on the specific types of PI and type of business.

- The Credit Information Use and Protection Act (CIPA) covers credit information, including financial and transaction data, and financial services reliant on such data. For financial sector businesses, processing of such data is also subject to the Electronic Financial Transactions Act (EFTA).
- For PI involving location data such as GPS data, there is the Act on the Protection, Use Etc of Location Information (LIPA).
- For IT service providers, which includes virtually any online business, there is also the Act on Promotion of Information and Communications Network Utilisation and Information Protection Etc (ITNA).
- For the cloud sector, data protection aspects are addressed partly in the Act on the Development of Cloud Computing and Protection of its Users, and, for the financial sector, in the EFTA.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Personal Information Protection Commission (PIPC) is the chief regulator. The PIPC has fairly broad powers to monitor and investigate PIPA compliance, and this can extend to a full-scale audit.

A large and visible role is played by the Korea Internet & Security Agency (KISA), the PIPC's monitoring arm. This includes periodic surveys, monitoring of the more popular online services and inquiries in follow-up to user complaints. KISA's findings and recommendations can escalate to decisions and enforcement steps by the PIPC.

The Korea Communications Commission (KCC) monitors compliance with ITNA, which extends to issues such as smartphone data access and online illicit video content, and with LIPA, concerning the use of location information.

The PIPC and the KCC have the power to impose administrative fines and corrective orders.

CIPA and EFTA are mainly administered by financial regulators, chief of which is the Financial Services Commission.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The PIPC has a general task of coordinating data privacy policy among government agencies, and it cooperates with the KCC, the financial regulator and other departments, such as the Ministry of Science and ICT in relation to technology and the Ministry of Health and Welfare in relation to the life sciences sector. Important guidelines are drawn up by the agencies in cooperation with each other.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Violations of PIPA, as well as the other PI governing statutes, can result in administrative fines, generally in the range of 10 million won to 50 million won. Regulators can also impose corrective or remediation orders, including orders to fix the infringing practice or, at the extreme, to suspend the PI handling activity pending remediation.

Revenue-based administrative fines can apply in cases of non-consensual use of PI and other infractions of a relatively serious kind. The PIPC may impose fines of up to 3 per cent of the annual revenues relating to the non-compliant conduct, where, for example, a PI controller, without due consent (separate or special consent as applicable), uses or transfers PI, collects sensitive information or collects the PI of children under age 14; or where it suffers a PI leakage, theft, loss or other such event, having failed to observe due security precautions.

Criminal penalties, including potential prison time and fines, are applicable to the more egregious, invasive or impactful types of offences, such as profit-seeking and knowing misuse of PI.

Often, compliance scrutiny will lead to, first, a stage of one or more warnings and requests for modifications (shy of a binding corrective order) from the monitoring agency KISA, before possible escalation to the stage of PIPC review for formal, decisive action.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Determinations by the data privacy regulators (administrative fines and corrective orders) can be contested by administrative law proceedings in the courts.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Information Protection Act (PIPA) covers virtually all sectors and types of organisation, and applies to the public and private sectors. There are some exceptions, which are normally of little relevance for business.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

PIPA does not specially address such issues of surveillance, although it applies to any PI in that context. Surveillance is restricted under the Protection of Communications Secrets Act, which broadly prohibits wiretapping of, and interference with, telecoms or electronic communications without consent. Questions of interpretation of that statute intersect with PIPA when it comes to, for example, monitoring employee web traffic.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

The Credit Information Use and Protection Act and the Electronic Financial Transactions Act contain specific protections for individual credit data.

The Act on Promotion of Information and Communications Network Utilisation and Information Protection Etc (ITNA) applies generally to online or app-based services, including to app access to data stored on devices (smartphones).

The handling of medical records is governed by the Medical Service Act, which includes tight restrictions on transfers of treatment records. Medical research data is also restricted under the Bioethics and Safety Act.

PI formats

9 | What categories and types of PI are covered by the law?

PIPA applies to all PI. Naturally, many restrictions will be more important at scales of data that only arise electronically. However, in a number of respects, there are stricter rules for PI collection and use by online services, and there are specific rules that apply to those services. For example, data incident reporting is stricter for online services, and potential penalties for PIPA violations include, for online services, a fine calculated as a percentage (3 per cent) of related revenue.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

PIPA is not confined in its reach to PI controllers and processors physically present in Korea. PIPA does not specifically provide for extra-territorial reach, but it, as well as the other main laws, can apply, and in important respects it is understood by the regulators to apply, to the processing of PI of Korean individuals wherever the processing is done. In general, in the online sphere, whether a service will be seen as subject to PIPA depends partly on its local user numbers and on issues such as whether it offers its service in the Korean language or houses data on a local server.

As a parameter for offshore processing of big data, the anonymisation of PI (not to be confused with pseudonymisation) renders it no longer PI, meaning it is no longer subject to PIPA.

There is a requirement to appoint a local representative: online service providers that lack a presence in Korea, while meeting certain thresholds of scale in their local revenue and users, are required under PIPA (and ITNA) to appoint a local representative, for the role of fielding official inquiries and user complaints relating to PI handling. Among the thresholds, this requirement applies if the offshore business has, for example, a total worldwide revenue of over 1 trillion won or over 1 million Korean users (in terms of PI stored) as a daily average. The local representative is often a professional agency or a local affiliate of the service provider. For certain of the largest services, it must effectively be a local subsidiary, if there is one, starting in late 2022.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

PIPA covers virtually every kind of use and processing of PI. The term 'processing', used throughout the statute, is defined to cover the collection, use, value-added processing, editing, combination, storage and transfer, among other things, of PI.

When PI is pseudonymised, it remains PI but is subject to lesser constraints in several respects than in the pre-pseudonymised state – among other things, it is no longer subject to access requests from data subjects or the PIPA-required notification of a data breach to users. In contrast, when PI is anonymised (rendered infeasible to reidentify), it is no longer PI and, thus, no longer governed by PIPA.

There are basic distinctions between controllers (or, more accurately translated, PI 'handlers') and processors (under PIPA, 'entrustees') of PI, along with data subjects (the individuals to whom the PI pertains). The PIPA terms 'handler' and 'entrustee' do not correspond exactly to 'controller' and 'processor', but the latter terms, used in the EU General Data Protection Regulation, work well enough in most PIPA contexts.

For PIPA purposes, the concept of owners of PI is not specially defined and, in most contexts, is not very useful to consider on top of controllers, processors and data subjects.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Korean law requires express opt-in consent, together with a significant range of disclosures set out in a privacy policy (or privacy notice). This is typically handled by presenting a set of consent confirmations in a checkbox format. The accompanying disclosures must include, among other things, the types of PI to be collected, the purposes, the retention periods and intended transferees, and a reminder of the right to withhold consent. Often, privacy policies of US- or EU-based multinationals fall short in a couple of these areas, especially in listing transferees.

Besides express consent, there are a few other valid bases for collecting PI, but usually these have only limited or interstitial relevance in business. One such basis, where there is an 'unavoidable need' to collect PI to enter into and fulfil a contract with the data subject, may sound like it should apply to many spheres of PI collection, but it is construed narrowly.

In general, it is not sufficient to rely on a perceived legitimate interest without getting express, opt-in consent. The Personal Information Protection Act (PIPA) includes a provision for the collection of PI based on legitimate or 'justifiable' interest, but this is viewed narrowly and does not come up regularly.

There are important exceptions to the consent requirement. Among these, under provisions added to PIPA in 2020, non-consensual use of PI in pseudonymised form is permissible for 'scientific research' purposes, which becomes important for commercial research and development.

Normally it does not suffice to simply obtain an affirmation that a user or customer agrees to or accepts the privacy policy as a whole. Rather, one must get specific consent for separate items. A typical consent window, in the Korean online sector, will include five or more checkboxes.

In addition to the main consent for the collection and processing of PI in accordance with the privacy policy, normally separate consents will need to be obtained for transfers of PI to other parties, PI transfers offshore, the use of PI for marketing purposes, the receipt of marketing messages and so on.

Each consent item must be expressly designated as mandatory (or necessary) or optional – in other words, necessary or not for the main functionalities of the service to work (thus, marketing-related items, for instance, are usually optional).

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Korean law imposes stricter rules in relation to several types of PI. Specific, separate opt-in consent is required for the collection and use of sensitive information, such as information about health and personal beliefs, and unique identifying information, including Korean ID numbers (resident registration numbers – a super-restricted subcategory, mostly off-limits even with consent), passport numbers and driver's licence numbers. Both of these categories, sensitive information and unique identifying information, come up in the internal HR context; PI-related consents obtained from employees typically include those added checkboxes.

Credit information – banking records and credit card transactions, etc – falls under the Credit Information Use and Protection Act and the Electronic Financial Transactions Act, and is subject to heightened security standards.

Medical records are restricted under the Medical Services Act, which, among other things, bars most transfers of records from the treating hospital or physician to any third party, failing an extremely cumbersome patient consent procedure.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

A data subject has general rights to access or obtain his or her PI that is with the PI controller, together with information concerning the use and transfer of that PI.

In addition, an IT service provider, basically any online service, must issue a notice to its users (assuming their PI includes contact information) at least once a year, if it meets a threshold of scale, namely either 10 billion won in online-sector revenues or 1 million PI-saved users on average in the fourth quarter of the prior year. The notice must describe the collection and use of the users' PI, including the purposes, items of PI and transferees.

As a separate point, under the Personal Information Protection Act (PIPA) a business that receives, for processing, PI from third parties (which transfer the PI based on consent from the data subjects) amounting to PI of 1 million or more data subjects must notify the data subjects of the receipt and intended processing of the PI.

Exemptions from transparency obligations

15 | When is notice not required?

PI access requests from data subjects can be put off based on 'justifiable grounds', but this is not well defined.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

There is an obligation, stated in a general way, to ensure that PI collected is accurate and up to date, to the extent necessary for the particular purposes. This general obligation seldom becomes a focal issue.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Data minimisation is included in PIPA's statement of cardinal principles: PI should be collected to the minimum extent necessary for the specific purposes and, moreover, PI should be anonymised or pseudonymised if the data in that state is good enough for the purpose.

A data controller must not refuse a service for lack of user consent to an unnecessary strand of PI collection; therefore, an app, for example, cannot require the user to consent to access to his or her data for marketing purposes that are not necessary for the main functionality.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Generally, PI must only be retained for so long as this is necessary for the purpose at issue, or as required under other laws, after which it must be destroyed or deleted. PIPA does not provide for specific retention periods, although it does require disclosure of the operative periods

to users (often merely phrased as 'until the information is no longer needed'). There are various minimum retention periods under other laws, such as five years for transaction or payment records under the Act on Consumer Protection in Electronic Commerce and the tax code.

Under the Act on Promotion of Information and Communications Network Utilisation and Information Protection Etc, for online services, there is a one-year limit on the PI of dormant users: if the user doesn't use the service for one year, the service must delete it or else keep and administer it separately from active users' PI.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

In general, PI can only be used for the purposes expressly consented to (ie, the purposes specified in the disclosures (privacy policy) accompanying the required consents). There are exceptions permitting the use of PI where specifically authorised by law or in emergencies.

Some latitude was seemingly added to PIPA in 2020, with new provisions allowing for the use or transfer of PI within a 'scope reasonably related' to the original, consented-to purposes, and provided that this is not detrimental to the data subject and is accompanied by due security measures. However, these provisions remain largely untested and are probably treated, for now, as at best a fallback when added consents are impractical to get.

In addition, since 2020, PIPA has permitted the use of PI in pseudonymised form for 'scientific research' (as well as 'statistical' and 'archival') purposes without additional consent. This has important implications for commercial research and development.

PIPA has always had a clause allowing for non-consensual PI collection and use based on a justifiable interest of the PI controller that is 'manifestly superior' to the data subject's rights. This clause is seldom relied on but can be relevant to, for example, investigation into suspected misconduct.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Korean law does not directly restrict this use of PI. Under the Credit Information Use and Protection Act, there is a related sort of restriction in the case of 'credit information companies', engaged in businesses such as credit scoring and investigation and debt collection-related services. Someone who has been the subject of automated decision-making by such a company is entitled to obtain an explanation of the result and challenge the result. The rule might justify complaints of wrongful profiling.

In a preliminary move towards the regulation of artificial intelligence (AI), the government has released a set of 'AI for Humanity' ethical standards for the development and use of AI, which point toward empowering individual voices and safeguarding against discrimination, for example, in the context of AI-driven processes. These high-level standards are non-binding, and definite rules in this vein probably have a long way to go.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

PI controllers are generally required to plan and implement organisational (or administrative) safeguards, as well as technical and physical safeguards. Important safeguards include the staffing of PI-related personnel, with role-appropriate allocations of data access and systems to maintain access logs.

As part of this, every PI handling enterprise in Korea is required to have a data privacy officer. Basic technical requirements include data access protocols and controls, encryption systems, firewalls, and anti-virus and anti-malware programs and systems.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Under the Personal Information Protection Act, in general, upon the occurrence of a data leakage, the data controller must 'without delay':

1 send notice of it to the affected individuals;
2 report it to the Personal Information Protection Commission (PIPC) (or the Korea Internet & Security Agency); and
3 post a notification on the data controller's homepage.

In the case of an online service, 'without delay' means within 24 hours of learning of the incident (together with the fact that it involves the PI of Korean individuals). Steps (2) and (3) do not apply if the company does not operate online and the data breach affects under 1,000 Korean individuals.

In addition to local data incidents, these rules apply to any offshore incident if it involves the PI of Korean individuals. The notice to the data subjects and the report to the PIPC must include, in addition to the particulars of the data breach, information on the remedial steps.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Data controllers have a general obligation to prepare and implement an internal data management plan, designed to prevent the loss or other impairment of PI (eg, theft, leakage, damage and unauthorised alteration). In addition to other safeguards (organisational, technical and physical), the plan must include preparatory and contingency plans for responses to data incidents and disaster scenarios, and measures to check up on PI handling by data processors.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

All data controllers must have a data protection officer (DPO) or a chief privacy officer. The DPO should be an executive or director or, failing that, the head of the PI control department.

The DPO's main areas of responsibility include data protection plans and systems, the privacy policy, the inspection and improvement of PI protection practices (including, at least, an annual check-up on the internal data management plan), related training, incident responses, compliance efforts and responses and, generally, the supervision of PI protection tasks and issues.

Intra-group appointment of a DPO is often the practical approach. For very small-scale businesses, the CEO (representative director) is deemed the DPO.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

A data controller must maintain the system access logs (covering data including PI accounts, access time records and PI processes carried out) and records of allocations of access authorisation among its personnel (access granted, modified or cancelled). These records must be retained for at least one to two years, depending on the number of data subjects and types of PI, or, with regard to access allocations, three years (five in the case of an online service).

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Public agencies are required to carry out privacy impact assessments concerning their handling of PI and submit these to the Personal Information Protection Commission. In the private sector, there is no special requirement of full-blown risk assessment processes as such. Evaluation of the risk and potential impact on PI systems is inherent in parts of the planning required of a company as a PI controller and on the part of its DPO.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

There is no particular obligation of privacy-by-design as such. There are various requirements under PIPA and other laws, such as those relating to data minimisation and technical security, that intersect with privacy-by-design concepts.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

PI controllers and processors as such are not required to register with the Personal Information Protection Commission or other data regulator.

Other transparency duties

29 | Are there any other public transparency duties?

There is no such duty in terms of a general transparency standard, apart from requirements to post a privacy policy and disclose various matters in conjunction with obtaining consents as required for PI collection and use.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

When a PI controller shares PI with third parties by way of outsourcing (ie, for fulfilment of the controller's services), this is termed 'entrustment' of PI to the third party (processor or entrustee). Entrustment requires:

1 disclosure to the data subjects, normally in the privacy policy, of the entrustees and the scope of outsourced work;
2 a data processing agreement (DPA) between the controller and the entrustee; and
3 some scope of ongoing precautions on the part of the controller.

The disclosure in point (1) must, strictly speaking, include the specific identities of entrustees.

The DPA must address a minimum scope of provisions, including specification of the purposes of entrustment and the corresponding scope of permitted use (and the prohibition of any other use), restrictions (if any) on further entrustment, data protection measures, provisions for controller supervision and inspection, and indemnification by the entrustee.

The controller is to carry out data protection-related education or instruction to, and supervision of, the entrustee.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Sharing of PI that is in the nature of (in EU General Data Protection Regulation terms) controller-to-controller transfers of PI – essentially, for the transferees' separate business purposes – is termed 'third-party provision' of PI under the Personal Information Protection Act (PIPA), and this requires explicit, opt-in consent from the data subjects. The consent must be accompanied by disclosures (normally offered in the privacy policy) of the identities of the transferees, types of PI and purposes of transfer, and the transferees' retention periods, and additional cumbersome details in the case of cross-border transfers by online service providers.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

Transfers of PI overseas are not restricted as a general category. However, when the transferring PI controller provides an online service, the transfer requires specific consent from the data subjects, separate from their general consent to PI collection, and coupled with disclosure of (on top of the usual matters) the country where the transferee is located, the contact information for the person in charge of data protection (or data protection officer) at the transferee, and the date and method of transfer.

If the overseas transfer is in the way of entrustment (ie, to a processor), obtaining consent is unnecessary if all those details are set out in the transferring PI controller's website-posted privacy policy. If

the transfer is a third-party provision of PI – controller-to-controller – it requires consent in any event, together with disclosures.

For many businesses, strict compliance with this framework can be difficult and even somewhat impractical.

Online service providers, in carrying out transfers overseas, must also require data security safeguards on the part of the transferees, reflecting this in contracts with them.

Further transfer

33 If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Where PI transfers overseas are subject to consent and disclosure requirements (in the case of cross-border transfers by IT service providers), under PIPA the offshore transferee is, in turn, subject to the same requirements for onwards transfer of PI to a third country. This is the case even if the transferee (the first one or any subsequent one) is not itself an IT service provider.

This framework can lead to complications in practice, considering, for instance, the fact that transferees are typically ill-placed to approach data subjects. There is a pending bill to amend PIPA that would probably ease the framework for transfers to the European Union, at least, by allowing PI transfers to jurisdictions that are deemed to provide comparable levels of PI protection.

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

Financial institutions are barred from transferring unique identifying information (resident registration numbers and passport numbers, etc) offshore. In addition, local financial institutions, in handling electronic financial transactions, are restricted from processing, on offshore cloud systems, personal credit information and unique identifying information.

RIGHTS OF INDIVIDUALS

Access

35 Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

A data subject has the right, upon request, to obtain his or her PI that is with the data controller, together with details including the uses of the PI, the use and retention periods, and transfers to third parties. Upon such a request, the controller must provide the information within 10 business days, but it can take longer if there are 'justifiable grounds' for delay. The data controller must allow such requests to come in by methods convenient to the data subjects and designate the methods on its website.

There are some limitations on this right to information, but they are relatively minor (eg, where access is, for some reason, legally prohibited). In practice, access requests are often handled by email exchanges; occasionally, online services offer online request and download.

Other rights

36 Do individuals have other substantive rights?

On viewing their PI, data subjects are generally entitled to request corrections to the PI, or to request deletion of it. They also have the right to request suspension of the use and processing. In the case of PI controllers that are IT service providers, a data subject may altogether withdraw (or rescind) consent to the collection, use and other processing of their PI (ie, opt out) easily and at any time, in which case the controller must promptly destroy the PI.

Compensation

37 Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Data subjects (the affected individuals) can claim monetary compensation against a PI controller under several different rubrics. The data subject can claim damages resulting from a violation of the Personal Information Protection Act (PIPA), unless the controller can prove it was not at fault (by intentional wrongdoing or negligence). Damages can include psychological harm, but that is typically hard to prove or quantify.

The data subject can, alternatively, seek compensation up to treble (ie, punitive) damages against the controller in the event of a loss, leakage, wrongful alteration or other such impairment of PI resulting from the fault of the controller (which has the burden of proving lack of fault). In assessing punitive damages, the court is to look at a variety of factors, including relevant gains to the controller and the controller's efforts to remedy the harm.

As a separate type of claim, the data subject can seek statutory damages of up to 3 million won.

The above framework for damages claims applies only to PIPA violations. Claims based on violations of other laws, such as the Credit Information Use and Protection Act or the Act on the Protection, Use Etc of Location Information, are possible but would come under the general Civil Code framework for claims for damages resulting from wrongful or negligent conduct.

Enforcement

38 Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights of access, correction, deletion, suspension and opting out are ultimately enforceable in the courts. Practically, the rights can also be effectuated by complaint to the Personal Information Protection Commission, for inquiry and eventual enforcement. Compensation claims go through the courts.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 Does the law include any derogations, exclusions or limitations other than those already described?

Several of the important requirements and restrictions do not apply to PI once it is pseudonymised, although as such it remains PI. This includes the obligation to destroy or delete PI once it is no longer needed for the stated purposes; the prompt notification and reporting of data leakages; and the rights of access by data subjects to PI, the correction or deletion of PI and the suspension of processing. These constraints do not apply to pseudonymised PI. On the other hand, the generation and processing of pseudonymised PI are subject to extensive guidelines.

While the Personal Information Protection Act applies to public as well as private sector collection and use of PI, there are broad exceptions concerning PI processing by public agencies, such as in a national security context.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Where cookies will be combined with other data to identify individuals, the use of the cookies as a tool for the 'automatic collection of PI' must be disclosed as part of the privacy policy, based on which the main opt-in consent for collection of PI must be obtained. It is not mandatory, however, to put a pop-up banner regarding the use of cookies or a stand-alone cookie policy.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

Sending marketing emails and text messages requires specific opt-in consent under the Act on Promotion of Information and Communications Network Utilisation and Information Protection Etc (ITNA) and the Personal Information Protection Act (PIPA). Further, overnight messages of this kind – between 9pm and 8am – require another specific consent. There are also format and content requirements, such as to include a salient 'advertisement' label in the email subject line, identify the sender and contact number, and include opt-out or unsubscribe details. In general, data protection rules and regulators tend to be especially guarded about marketing communications.

Targeted advertising

42 | Are there any rules on targeted online advertising?

The Personal Information Protection Guideline for Online Customised Advertising, promulgated by the Korea Communications Commission, provides a set of principles, mainly concerned with ample disclosures and control features. Among these guidelines, which are not binding, advertisers should:

- disclose, in the privacy policy, various features of the advertising and include the names of advertisers, the items of behavioural data collected, its purposes, retention periods and third-party access to the data;
- provide convenient opt-out and setting controls; and
- obtain particular consent for elements such as sensitive information.

The Personal Information Protection Commission (PIPC) is understood to be preparing, for promulgation in the near future, detailed guidelines on the use of customised advertising methods and tools, including the use of behavioural data, for tighter regulation of these practices within the PIPA framework. There are signs that the PIPC has, in 2022, already commenced significant enforcement efforts against certain of these practices.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

PIPA contains special provisions for processing 'sensitive' PI, chiefly a requirement of specific, opt-in consent (separate and in addition to the main consent for PI collection and use in accordance with the privacy policy). Sensitive PI of a data subject is defined under PIPA to include any beliefs and views, political affiliation, labour union background, health information, genetic testing results, criminal history and other categories of a distinctly personal nature.

bkl BAE, KIM & LEE

Kwang Hyun Ryoo
kh.ryoo@bkl.co.kr

Juho Yoon
juho.yoon@bkl.co.kr

Tae Uk Kang
taeuk.kang@bkl.co.kr

Minwoon Yang
minwoon.yang@bkl.co.kr

Minyoung Kim
minyoung.kim@bkl.co.kr

Centropolis B
26 Ujeongguk-ro
Jongno-gu
Seoul 03161
Korea
Tel: +82 2 3404 0000
www.bkl.co.kr

Profiling

44 | Are there any rules regarding individual profiling?

Korean data regulation does not include rules governing automated profiling as a category of PI use. However, in the case of credit rating agencies and other credit information companies, under the Credit Information Use and Protection Act, a person who has been the subject of an automated decision-making process by such an agency is entitled to question and challenge the result, and one potential basis for challenge would be an error or impropriety in profiling. There are some broad ethical standards for the development and use of artificial intelligence, announced in 2020, that acknowledge a need to avoid discrimination.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Cloud system security and stability are covered in the Act on Development of Cloud Computing and Protection of Users (the Cloud Computing Act) and the Electronic Financial Transactions Act, along with financial industry regulations and guidelines such as the Guidelines for Use of Cloud Computing Services in the Financial Sector. In this framework, cloud processing of individual customer credit and transaction records by financial businesses is subject to extensive security-related conditions, assessments and other safeguards, including rigid network separation conditions. However, the primary regulator, the Financial Services Commission, has announced plans to liberalise the framework soon, to some extent.

UPDATE AND TRENDS

Key developments of the past year

46 Are there any emerging trends or hot topics in international data protection in your jurisdiction?

There is a pending bill to amend the Personal Information Protection Act (PIPA) that would significantly impact many aspects of the regulations. The bill has passed all major hurdles of review prior to a submission for vote in the legislature, and it is widely expected, mostly in its current draft state, to be passed into law in 2022, likely taking effect in 2023. If passed, PIPA would be amended in the following ways:

- The potential revenue-based administrative fine, for various serious kinds of violations in the online sector, would be up to 3 per cent of total revenue (as opposed to just violation-related revenue).
- PI controllers would have more leeway to transfer PI offshore without specific consent, such as where the destination country is deemed to satisfy PIPA levels of data protection. At the same time, PIPA would augment the Personal Information Protection Commission's power to suspend non-compliant PI transfers offshore.
- PIPA would require an entrustee (processor) to obtain the PI controller's consent before re-entrusting the data to a further entrustee.
- PIPA would provide a significant range of data portability rights.
- Data subjects would have some degree of rights to opt out of the use of their PI in AI-powered decision-making.
- Data controllers in general would be required to accede to dispute resolution with the Personal Information Dispute Mediation Committee.

In a separate development, the Financial Services Commission, the primary financial regulator, announced in April 2022 that it plans to modify the current, highly restrictive framework for use of cloud systems in the financial sector. As outlined, the plan would include steps to simplify security criteria and apply different standards varying with the type of cloud processing. Network separation requirements would also be reassessed. Initial steps, including a revised set of guidelines, are expected by late 2022.

Switzerland

Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Switzerland has dedicated data protection laws. On the federal level the Federal Data Protection Act (DPA), together with the Ordinance to the DPA (DPO), governs the processing of what in Switzerland is called 'personal data' (PI) by private parties or federal bodies. Processing of PI by cantonal authorities (cantons are the Swiss states) is subject to state legislation, which will not be discussed here.

Additionally, several other federal laws contain provisions on data protection, especially laws that apply in regulated industries (eg, financial markets and telecommunications), which further address the collection and processing of PI:

- the Swiss Code of Obligations sets forth restrictions on the processing of employee data, and Ordinance 3 to the Federal Employment Act limits the use of surveillance and control systems by the employer;
- the Federal Telecommunications Act regulates the use of cookies;
- the Federal Unfair Competition Act regulates unsolicited mass advertising through electronic communications such as email and text messages;
- statutory secrecy obligations, such as banking secrecy (outlined in the Federal Banking Act (the Banking Act)), financial institutions secrecy (outlined in the Federal Act on Financial Institutions (the Financial Institutions Act)), financial market infrastructure secrecy (outlined in the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (the Financial Market Infrastructure Act)) and telecommunications secrecy (outlined in the Telecommunication Act) apply in addition to the DPA;
- in the financial industry, the Banking Act, the Financial Institutions Act, the Financial Market Infrastructure Act and the Federal Act on Combating Money Laundering and Terrorist Financing stipulate specific duties to retain and disclose information;
- in the telecommunications industry, the Telecommunication Act and the Federal Act on the Surveillance of Post and Telecommunications stipulate specific duties to retain and disclose information; and
- the Federal Act on Research involving Human Beings (and the corresponding ordinance), the Federal Act on Human Genetic Testing (and the corresponding ordinance), the Federal Act on Electronic Patient Records (and the corresponding ordinance), the Federal Act on Medicinal Products and Medical Devices, the Federal Act on Combatting Contagious Human Diseases and the Federal Act on Registration of Cancer Diseases set out specific requirements for the processing of health-related data.

Switzerland is a signatory to certain international treaties regarding data protection, such as the European Convention on Human Rights and Fundamental Freedoms and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention 108) and its additional protocol of 8 November 2001.

Although Switzerland is not a member of the European Union and, hence, is not directly subject to EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), it has been officially recognised by the European Commission as providing an adequate level of protection for data transfers from the European Union.

The revised DPA, which was already adopted by the Swiss parliament in September 2020 and will presumably enter into force by 1 September 2023, aligns Swiss data protection law with international rules on data protection to comply with the revised Convention 108 and the GDPR. This will hopefully allow Switzerland to uphold its status as a country adequately protecting PI from an EU perspective, which allows for easier transfer of PI from the European Union and the ratification of the revised Convention 108.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Federal Data Protection and Information Commissioner (FDPIC) is the federal data protection authority in Switzerland. Also, cantons are competent to establish their own data protection authorities for the supervision of data processing by cantonal and communal bodies.

The FDPIC has no direct enforcement or sanctioning powers against private bodies processing PI. Nevertheless, the FDPIC can carry out investigations on its own initiative or at the request of a third party if methods of processing are capable of violating the privacy of a large number of persons (eg, system errors), if data collections must be registered or if there is a duty to provide information in connection with a cross-border data transfer. To this effect, the FDPIC may request documents, make inquiries and attend data processing demonstrations. Based on these investigations, the FDPIC may recommend that a certain method of data processing be changed or abandoned. However, these recommendations are not binding.

Under the revised DPA, the FDPIC initiates, ex officio or upon notification, an investigation if there are sufficient indications that specific data processing activities could violate data protection rules (unless such violation is of minor significance), and should such investigation reveal a violation, render binding administrative measures, including that:

- processing is fully or partially adjusted, suspended or terminated;
- PI is fully or partially deleted or destroyed; and

- in certain cases, disclosure abroad is deferred or prohibited.

In contrast to most other European data protection authorities, the FDPIC still cannot impose any (administrative) fines.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The FDPIC may cooperate with domestic and foreign data protection authorities. This includes a general professional exchange with such authorities related to certain specialist areas or regular cooperation within committees, working groups, conferences, etc. However, the FDPIC does not have a mandate or competence to collaborate with other data protection authorities (whether domestic or foreign) concerning supervision and control of processing activities or to share information with them. A collaboration of the FDPIC with foreign data protection authorities concerning data processing in specific cases may (except for data processing related to judicial and police cooperation or Schengen law respectively) be particularly difficult, as in general, the ordinary course of international judicial assistance must be followed (subject to applicable specific laws).

Certain exceptions to the above rule apply within the applicability of the Schengen law, whereby the Ordinance on the national part of the Schengen Information System and the SIRENE Bureau (the N-SIS-Ordinance) explicitly foresees a collaboration of the FDPIC with Swiss cantonal data protection authorities concerning coordinated supervision of PI processing, all in accordance with their respective competences. The N-SIS-Ordinance provides further that the FDPIC in performing its tasks shall closely work together with and serve as a national point of contact for the European Data Protection Supervisor.

Under the revised DPA, federal and cantonal authorities must provide the FDPIC with the information and PI required for the performance of his or her statutory duties. The FDPIC discloses information and PI required for the performance of the statutory duties of:

- Swiss authorities responsible for data protection;
- competent criminal prosecution authorities, in certain instances; or
- federal authorities as well as cantonal and communal police forces for the enforcement of certain data protection related measures.

Further, under the revised DPA, the FDPIC may exchange information and PI with foreign competent data protection authorities for the performance of their respective statutory data protection duties, if:

- reciprocity of administrative assistance is ensured;
- information and PI are only used for the data protection related proceedings forming the basis of the request for administrative assistance;
- the receiving authority undertakes to keep professional, business and manufacturing secrets confidential;
- information and PI are only disclosed to third parties with the transmitting authority's prior approval; and
- the receiving authority undertakes to adhere to the conditions and restrictions imposed by the transmitting authority.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Violations of the data protection principles are generally not criminally sanctioned. However, private parties are liable to a fine of up to 10,000 Swiss francs if he or she wilfully:

- fails to provide information concerning safeguards in the case of cross-border data transfers;
- fails to notify data collections;
- provides information concerning safeguards or notification of data collections and in doing so wilfully provides false information; or
- provides the FDPIC with false information in the course of an investigation or refuses to cooperate.

Also, wilfully carrying out the following actions is punishable by a fine of up to 10,000 Swiss francs upon a complaint:

- refusing to permit a data subject access to their PI or providing him or her with wrong or incomplete information (ie, violating the data subject's right of access);
- failing to inform a data subject about the collection of sensitive PI or personality profiles; and
- failure by certain professionals to keep sensitive PI and personality profiles confidential.

Under the revised DPA, the wilful violations set out above (and many further violations) are subject to a fine of up to 250,000 Swiss francs. Further, professional secrecy will not be limited to the usual bearers of professional secrets but will arguably extend to any profession for which protection of confidentiality of 'secret' PI is essential. Violations of the data protection principles, however, are still not criminally sanctioned.

1.5 Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

The FDPIC can carry out investigations under certain circumstances and, based thereon, issue recommendations that are non-binding; hence, there is no need for them to be reviewed by a judicial body. If a recommendation made by the FDPIC is not complied with or is rejected, the FDPIC may refer the matter to the Federal Administrative Court for a decision. The verdicts of the Federal Administrative Court are appealable to the Federal Supreme Court (for a final ruling) both by the FDPIC and the defendant.

Under the revised DPA, the FDPIC may, following an investigation revealing a violation of data protection rules, render binding administrative measures (ie, decisions or orders). The FDPIC's investigative proceedings and subsequent decisions or orders are governed by the Federal Act on Administrative Procedure. Only the federal body or private party against whom the investigations were initiated (but not the data subjects concerned) is a party to such proceedings. The FDPIC (and the federal body or private party) may, however, appeal against the Federal Administrative Court's appeal decision to the Federal Supreme Court for a final ruling.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Federal Data Protection Act (DPA) does not apply to:

- deliberations of the Federal Parliament and parliamentary committees;
- pending civil proceedings, criminal proceedings, international mutual assistance proceedings and proceedings under constitutional or administrative law, except for administrative proceedings of first instance;
- public registers based on private law;

- PI processed by state and communal bodies (regulated on the state level); and
- PI processed by the International Committee of the Red Cross.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The DPA does not cover the interception of communications, electronic marketing or monitoring and surveillance. These issues are dealt with in the following laws:

- the Swiss Federal Telecommunications Act;
- the Swiss Federal Act on Surveillance of Post and Telecommunications;
- the Swiss Federal Act on the Intelligence Service;
- the Swiss Federal Unfair Competition Act;
- the Swiss Code of Obligations; and
- Ordinance 3 to the Swiss Federal Employment Act, regarding employee monitoring.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Additional regulations concerning PI protection can be found in the following laws:

- the Swiss Constitution;
- the Swiss Civil Code;
- the Federal Act on Consumer Credits;
- Ordinance 3 to the Federal Employment Act (regarding employee monitoring);
- various laws, ordinances and other rules concerning data processing in the financial industry; and
- various laws and ordinances concerning the processing of health data.

Further regulations may apply depending on the given subject matter.

PI formats

9 | What categories and types of PI are covered by the law?

The DPA and the Ordinance to the DPA (DPO) apply to any data relating to an identified or identifiable person (individual or legal entity), irrespective of its form. A person is identifiable if a third party having access to the data on the person can identify such person with reasonable effort.

Under the revised DPA, the protection of PI relating to legal entities is removed to ease cross-border disclosure to jurisdictions that do not protect respective PI.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The DPA applies to any PI processing that occurs within Switzerland. Also, if a Swiss court decides on a violation of privacy by the media or other means of public information (eg, the internet), the DPA may apply (even if the violating PI processing occurred outside Switzerland) if the data subject whose privacy was violated chooses Swiss law to be applied. Swiss law may be chosen as the applicable law if:

- the data subject has his or her usual place of residence in Switzerland (provided the violator should have expected the results of the violation to occur in Switzerland);
- the privacy violator has a business establishment or usual place of residence in Switzerland; or
- the result of the violation of privacy occurs in Switzerland (provided the violator should have expected the results of the violation to occur in Switzerland).

The revised DPA explicitly states that it applies to facts that have an effect in Switzerland, even if they occur outside Switzerland, and that civil law claims are governed by the Federal Act on International Private Law (subject to any provisions on the territorial scope of the Swiss Criminal Code).

Further, under the revised DPA, controllers with domicile (or residence) abroad must designate a representative in Switzerland if they process PI of persons in Switzerland and such data processing:

- is related to the offering of goods or services or to the monitoring of their behaviour;
- is extensive;
- occurs regularly; and
- involves a high risk to the personality of the data subjects.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The DPA applies to any processing of PI. 'Processing' is defined in the DPA as any operation with PI irrespective of the means applied and the procedure. In particular, processing includes the collection, storage, use, revision, disclosure, archiving or destruction of PI. An exemption is made for PI that is processed by an individual exclusively for personal use and is not disclosed to third parties.

Unlike in EU countries, there is no specific distinction between owners of a data collection (ie, controllers) and mere processors. All persons or entities processing PI are equally subject to the provisions in the DPA and the DPO and have to adhere to the rules set out therein.

The revised DPA introduces a distinction between controllers and processors and attributes duties and responsibilities to each of them separately.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

PI must always be processed (this includes its holding) lawfully. The processing is lawful if it is either processed in compliance with the general principles set out in the Federal Data Protection Act (DPA) or non-compliance with these general principles is justified. The disclosure of PI to third parties is generally lawful under the same conditions. The principles set out in the DPA are:

- PI must be processed lawfully;
- the processing must be carried out in good faith and must be proportionate;
- the collection of PI and, in particular, the purpose of its processing, must be evident to the data subject at the time of collection;

- PI may only be processed for the purpose indicated at the time of collection, which is evident from the circumstances, or that is provided for by law;
- anyone who processes PI must ensure it is accurate;
- PI must be protected against unauthorised processing through adequate technical and organisational measures;
- PI must not be transferred outside Switzerland if the privacy of the data subjects would thereby be seriously endangered, in particular, due to the absence of legislation that guarantees adequate protection; and
- PI must not be processed against the explicit will of the data subject.

Non-compliance with these principles may be justified by:
- the data subject's consent (given voluntarily and after adequate information);
- the law (eg, duty to disclose information as required under financial market laws); or
- an overriding private or public interest.

According to the DPA, the overriding interest of the person processing the PI can, in particular, be considered if that person:
- processes PI directly related to the conclusion or the performance of a contract and the PI is that of the contractual party;
- processes PI about competitors without disclosing it to third parties;
- processes PI that is neither sensitive PI nor a personality profile to verify the creditworthiness of the data subject provided that such data is only disclosed to third parties if it is required for the conclusion or the performance of a contract with the data subject;
- processes PI on a professional basis exclusively for publication in the edited section of a periodically published medium;
- processes PI for purposes not relating to a specific person, in particular for research, planning statistics, etc, provided that the results are published in such a manner that the data subject may not be identified; and
- collects PI on a person of public interest, provided the data relates to the public activities of that person.

Under the revised DPA (and in contrast to EU Regulation (EU) 2016/679 (the General Data Protection Regulation)), such general concept will not change, ie, processing under the general data processing principles generally remains permitted. A justification (eg, consent or overriding interests) is only required in the case PI is processed contrary to the general data processing principles.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

In addition to 'normal' PI, the DPA introduced 'sensitive PI' and 'personality profiles' as special categories of PI that are subject to stricter processing conditions. Sensitive PI is data on:
- religious, ideological, political or trade union-related views or activities;
- health, the intimate sphere or the racial origin;
- social security measures; or
- administrative or criminal proceedings and sanctions.

A personality profile is a collection of PI that permits an assessment of essential characteristics of the personality of an individual.

Certain restrictions apply to the processing of sensitive PI and personality profiles in addition to the general principles:
- the reasons that serve as justification to process such data in violation of the general principles are more limited (eg, consent may only be given explicitly, not implicitly);
- disclosure – even if in compliance with the general principles – requires justification; and
- additional requirements depending on the specific case (eg, information duties, obligations to register data collections).

Also, there are more stringent rules in certain subject matters, such as employment law, health, telecommunications, finance and such like.

Under the revised DPA, genetic data and biometric data (which unequivocally identify an individual) are added to the definition of sensitive PI. Further, extensive processing of sensitive PI is determined to be likely to lead to a high risk to an individual's personality or fundamental rights and thus, requires the performance of a data protection impact assessment.

The revised DPA no longer features personality profiles as a special category of PI. Instead, high-risk profiling (ie, any form of automated PI processing to use such data to assess certain personal aspects relating to an individual that involves a high risk to the personality or fundamental rights of the individual, as it pairs data that enables an assessment of essential aspects of the personality of such individual) requires explicit consent by data subjects concerned.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Generally, it suffices if the collection of PI and, in particular, the purpose of its processing, is evident to the data subjects from the circumstance of collection. However, in the case of collection of sensitive PI or personality profiles, the owner of such collection is obliged to actively inform the data subject at least of the following:
- the identity of the owner of the data collection;
- the purpose of the data processing; and
- the categories of data recipients if the disclosure is intended.

This duty to actively provide information also applies if the data is collected from third parties.

The data subject has to be informed before the PI is collected. If the data is not collected from the data subject, the data subject must be informed at the latest when the data is stored or if the data is not stored, on its first disclosure. The information does not have to be provided in a specific form. For evidentiary purposes, however, the information should be provided in writing or another recordable form.

Under the revised Federal Data Protection Act (DPA), the requirements on transparent information to data subjects are extended significantly (to align them to EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR)) such that active information duties, in general, apply in any instance in which any PI (not just sensitive PI) is processed. In essence, data subjects must (at the time of collection) be informed about the controller's identity and contact information; the purpose of the processing; the identity of recipients (or the categories of recipients) in the case of disclosure to third parties; and the jurisdiction where the data is transferred to and safeguards implemented, as applicable, in the case of cross-border disclosure. Although mostly in line with the GDPR, the revised DPA also requires disclosure of every single jurisdiction where PI is being transferred to. Further, the data subject must be informed about automated individual decisions.

Exemptions from transparency obligations

15 | When is notice not required?

There are certain exceptions to this duty to inform, for example, if providing the information would result in the violation of overriding interests of third parties or if the data collection owner's overriding interests justify not informing the data subject (in the latter case this exception only applies if the PI is not shared with third parties).

If the PI has not been obtained directly from the data subject, but rather from a third party, the owner of the data collection must, nevertheless, provide the information stated above, except if:

- the data subject has already been informed thereof;
- the storage or disclosure is expressly provided for by law; or
- the provision of information is not possible at all, or only with disproportionate inconvenience or expense.

Similar exceptions apply under the revised DPA.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Anyone who processes PI must ensure that the data is accurate and take all reasonable measures to ensure that PI, which, given the purpose of its collection is or has become incorrect or incomplete, is either corrected or destroyed.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Other than the general principle that the processing of PI must be proportionate, there are no specific rules on the volume or types of PI that may be collected (at least as regards private parties – special rules apply to federal bodies as regards collection of sensitive PI); however, regular processing of sensitive PI or personality profiles requires registration of the data collection with the Federal Data Protection and Information Commissioner. According to this principle, processing may only be conducted if it is necessary and fits the purpose for which PI is processed. The same applies to the types and volume of PI. Accordingly, the permitted types and volume must be assessed on a case-by-case basis.

Under the revised DPA, PI must be destroyed or anonymised as soon as it is no longer needed for the purpose of the data processing, and extensive processing of sensitive PI requires a data protection impact assessment.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Other than the general principle that processing of PI must be proportionate (ie, processing may only be conducted if it is necessary and fits the purpose for which PI is processed), which also applies to the amount and length of time of holding PI, there are no specific rules on the amount or length of time. Accordingly, the permitted amount and length of time of holding PI must be assessed on a case-by-case basis.

Under the revised DPA, PI must be destroyed or anonymised as soon as it is no longer needed for the purpose of the data processing.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

According to the DPA, PI may only be processed for the purpose stated or evident at the time of collection or that is provided for by law. The processing purpose must be identifiable to the data subject.

Under the revised DPA, PI may only be obtained for a specific purpose that is identifiable to the data subject and such PI may only be processed in such a manner that is compatible with this purpose.

Use of PI for other purposes than those stated or apparent at the time of collection or provided for by law constitutes a breach of a general principle of the DPA, which is only permissible in the case of appropriate justification. This principle remains unchanged under the revised DPA.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

There are no rules on automated decision-making in the DPA.

Under the revised DPA, however, the data subject must be informed about automated individual decisions (ie, any decisions solely based on automated data processing and having legal effects or significantly affecting him or her), whereby the affected individual may generally request to express his or her point of view and have the decision reviewed by a person. The foregoing does not apply if:

- the automated individual decision is directly related to the conclusion or performance of a contract between the controller and the data subject, and the data subject's request is granted; or
- the data subject has expressly consented to the decision being automated.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

PI must be protected by appropriate technical and organisational measures against unauthorised processing. Anyone processing PI or providing a data communication network must ensure the protection against unauthorised access, the availability and the integrity of the data. In particular, the PI must be protected against the following risks:

- unauthorised or accidental destruction;
- accidental loss;
- technical faults;
- forgery, theft or unlawful use; and
- the unauthorised alteration, copying, access or other unauthorised processing.

The technical and organisational measures must be adequate and must be reviewed periodically. In particular, the following criteria must be considered:

- the purpose of the data processing;
- the nature and extent of the data processing;
- an assessment of the possible risks to the data subjects; and
- the current state of the art (especially currently available technology).

Concerning automated data processing, the owner of the data collection must take the appropriate technical and organisational measures to achieve, in particular, the following goals:

- data access control – unauthorised persons must be denied access to facilities in which PI is being processed;
- PI carrier control – preventing unauthorised persons from reading, copying, altering or removing data carriers;
- transport control;
- disclosure control – data recipients to whom PI is disclosed through devices for data transmission must be identifiable;
- storage control;
- access control – the access by authorised persons must be limited to the PI that they require to fulfil their task; and
- input control – in automated systems, it must be possible to carry out a retrospective examination of what PI was entered at what time and by which person.

The revised Federal Data Protection Act (DPA) provides that the technical and organisational measures must enable controllers and processors to avoid breaches of data security (ie, security breaches leading to unintentional or unlawful losses, deletions, destructions or modifications of PI or disclosure or accessibility of PI to unauthorised persons).

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There is no general or sector-specific data security breach notification obligation under Swiss data protection law. As a rule, it would contravene the general principles of tort law to provide for an obligation of the violator to proactively inform the damaged person or persons. Nevertheless, the Federal Data Protection and Information Commissioner (FDPIC) has advised lawmakers to oblige providers of social networking sites to inform data subjects of data breaches.

Special rules may apply in regulated markets (eg, a duty to notify the Swiss Financial Market Supervisory Authority FINMA of data breaches suffered by supervised entities or individuals).

The revised DPA introduces an explicit data breach notification obligation and defines a 'data breach' as a breach of security that results in PI being inadvertently or unlawfully lost, deleted, destroyed, altered or disclosed or made accessible to unauthorised persons. Data breaches that are likely to lead to a high risk to the personality or fundamental rights of the individual concerned must be notified to the FDPIC as quickly as possible. Where necessary for the protection of the individual or if requested by the FDPIC, the controller must also notify the affected individual. Contrary to EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (where data breaches must – where feasible – be notified to the supervisory authority within 72 hours unless the breach is unlikely to result in a risk to the individual's rights and freedoms), the revised DPA does not provide for a firm deadline.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Neither the Federal Data Protection Act (DPA) nor the revised DPA provide for any such explicit obligations to implement internal controls to ensure responsibility and accountability or to demonstrate compliance, except in:

- the general data processing obligations, which in various instances entail certain documentation (and, if a data collection must be registered with the FDPIC, include drawing up processing regulations inter alia describing the internal organization as well as data processing and control procedures);
- the obligation to implement suitable technical and organisational measures to ensure an appropriate level of data security; and
- under the revised DPA – the obligation to implement data processing technically and organisationally in such a manner that the data protection provisions are complied with.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The appointment of a data protection officer is not mandatory in Switzerland. However, the registration of data collections is not required if the owner of a data collection has appointed a data protection officer that independently monitors data protection compliance within the owner's business organisation and maintains a list of data collections.

The data protection officer must have the necessary knowledge of:

- Swiss data protection law and how it is applied in practice;
- the information technology and technical standards applied by the owner of the data collection; and
- the organisational structure of the owner of the data collection and the particularities of the data processing performed by the owner of the data collection.

The appointment of a data protection officer will only result in a release of the duty to register data collections if the Federal Data Protection and Information Commissioner (FDPIC) is notified of the appointment of a data protection officer. A list of such business organisations that have appointed a data protection officer is publicly accessible on the FDPIC's website.

The data protection officer has two main duties. First, the data protection officer audits the processing of PI within the organisation and recommends corrective measures if he or she finds that the data protection regulations have been violated. He or she must not only assess compliance of the data processing with the data protection requirements on specific occasions, but also periodically. Auditing involves an assessment of whether the processes and systems for data processing fulfil the data protection requirements, and whether these processes and systems are enforced in practice. If the data protection officer takes note of a violation of data protection regulations, he or she must recommend corrective measures to the responsible persons within the organisation and advise them on how to avoid such violations in the future. The data protection officer does not, however, need to have direct instruction rights.

Second, the data protection officer maintains a list of the data collections that would be subject to registration with the FDPIC. The list must be kept up to date. Unlike the data collections registered with the FDPIC, the internal data collections do not have to be maintained electronically nor must they be available online. However, they must be made available on request to the FDPIC and data subjects.

The data protection officer must:

- carry out his or her duties independently and without instructions from the owner of the data collections;
- have the resources required to fulfil his or her duties; and

- have access to all data collections and all data processing, as well as to all information that he or she requires to fulfil his or her duties.

There is no particular protection against the dismissal of the data protection officer. The data protection officer can be an employee of the data controller or an external person.

Under the revised DPA, to the extent a data protection adviser (who meets certain prerequisites set out in the revised DPA) has been appointed, the consultation of such data protection adviser may substitute the otherwise required consultation of the FDPIC following a data protection impact assessment, as applicable. The controller must notify the FDPIC and publish the contact details of the data protection adviser to benefit from the foregoing.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Although the owner of a data collection may have to provide available information about the source of collected data to comply with data subjects' right of access, there is no obligation to keep the relevant records. However, if such information would be deleted upon receiving an inquiry by a data subject, this could be deemed to be breaching the principle of good faith.

The revised DPA introduces a general duty to maintain records of processing activities (which is generally modelled after the corresponding obligation under EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR)) containing all relevant information and at least such information explicitly set out in the revised DPA. Controllers and processors must maintain records of data processing activities under their respective responsibility. Exemptions apply for companies with less than 250 employees in the case of low-risk data processing. In comparison, the GDPR's relief from maintaining data processing records only applies if – further to the above-mentioned prerequisites – data are only processed occasionally and no special categories of data or data relating to criminal convictions and offences are processed.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

There are no rules on carrying out risk assessments in the DPA.

Under the revised DPA, however, controllers must perform a data protection impact assessment (DPIA) whenever it appears that an envisaged data processing activity is likely to lead to a high risk to an individual's personality or fundamental rights (eg, in the case of extensive processing of sensitive PI or systematic monitoring of public areas).

The DPIA contains a description of the planned processing, an assessment of the risks to the personality or fundamental rights of the data subject and the protective measures to be taken.

The controller must generally consult with the FDPIC before such processing if the DPIA indicates that the contemplated processing may be of a high-risk nature despite any measures taken (unless a data protection adviser meeting certain statutory requirements has already been consulted).

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

In general, PI must be protected against unauthorised processing through adequate technical and organisational measures; however, there is currently no obligation to adopt privacy by design or by default.

The revised DPA introduces the concepts of privacy by design and by default, namely:

- setting up technical and organisational measures to meet data protection regulations and data processing principles from the planning of the processing, which shall be appropriate concerning the state of the art, type and extent of processing and associated risks; and
- ensuring through appropriate predefined settings that data processing is limited to the minimum required by the purpose unless the data subject instructs otherwise.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

The owner of a data collection that regularly processes sensitive PI or personality profiles, or regularly discloses PI to third parties, must register such data collection with the Federal Data Protection and Information Commissioner (FDPIC).

A data processor that transfers PI outside Switzerland is, under certain circumstances, obliged to notify the FDPIC of the data protection safeguards put in place.

The owner of a data collection is not required to register a data collection if:

- he or she processes PI owing to a statutory obligation;
- he or she uses the PI exclusively for publication in the edited section of a periodically published medium and does not pass any data to third parties without prior information;
- he or she has designated a data protection officer;
- he or she has acquired a data protection quality mark under a certification procedure; or
- it falls within a list of further exceptions by the Federal Council set out in the Ordinance to the DPA, including, among other things:
  - data collections of suppliers or customers, provided they do not contain any sensitive PI or personality profiles;
  - collections of PI that are used exclusively for research, planning and statistical purposes; and
  - accounting records.

In the case of a registration obligation, the collection must be registered before it is created, and the FDPIC must be informed by the owner of the data collection about:

- his or her name and address;
- the name and complete designation of the data collection;
- the person against whom the right of access may be asserted;
- the purpose of the data collection;
- the categories of PI processed;
- the categories of data recipients; and
- the categories of persons participating in the data collection, namely, third parties who are permitted to enter and modify PI in the data collection.

The owner of the data collection is under the obligation to keep the data collection registration up to date. Registration is available online. No fees are charged for the registration of a data collection.

Private parties are, as owners of a data collection, subject to a fine of up to 10,000 Swiss francs if:

- they wilfully fail to register the data collection;
- they wilfully provide false information in registering the data collection; or
- they wilfully and continuously fail to update the registration information.

Under the revised Federal Data Protection Act (DPA), the duty to notify data collections to (and register with) the FDPIC is (at least for private parties) abolished and replaced by the general obligation to keep records of data processing activities.

Other transparency duties

29 | Are there any other public transparency duties?

The database of data collections registered with the FDPIC is publicly available and can be accessed by anyone free of charge online. On request, the FDPIC also provides paper extracts free of charge. Other than the registration of a data collection or the notification to and publication by the FDPIC of the appointment of a data protection officer, as applicable, there are no public transparency duties under Swiss data protection law.

The appointment of a data protection officer results in a release of the duty to register data collections with the FDPIC provided the FDPIC is notified of such an appointment. A list of respective companies and organisations that have appointed a data protection officer is publicly accessible on the FDPIC's website.

The appointment of a data protection adviser under the revised DPA may lead to a release of the duty to consult with the FDPIC following a data protection impact assessment, as applicable, provided the data protection adviser's contact details are notified to the FDPIC and published and such data protection adviser has been consulted. It remains to be seen whether the FDPIC will also make available on its website a list of all companies and organisations that have appointed a data protection adviser under the revised DPA.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The processing of PI may be transferred to a third party if the transferor ensures that the third party will only process data in a way that the transferor is itself entitled to and if no statutory or contractual secrecy obligations prohibit the processing by third parties. The transferor must ensure that the third party will comply with the applicable data security standards.

Although this is not a statutory requirement, data processing should be outsourced to third parties by written agreement only. Such agreement will typically require the third party to process the PI solely for the purposes and only under the instructions of the transferor.

Under the revised Federal Data Protection Act (DPA), data subjects must be informed about the identity or categories of recipients in the case of disclosure to third parties. Further, a processor may no longer engage a sub-processor without the prior consent of the controller. However, in contrast to EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), the revised DPA does not prescribe any (minimum) content for a data processing agreement.

Special rules may apply in regulated markets. Circular 2018/03 issued by the Swiss Financial Market Supervisory Authority FINMA (Outsourcing Circular) applies to banks (including holders of a fintech licence), insurers, reinsurers, securities firms, managers of collective assets with a registered office in Switzerland and Swiss branches of foreign banks, insurers, securities firms and managers of collective assets, as well as fund management companies (with registered office and a head office in Switzerland) and self-managed investment companies with variable capital. Before outsourcing a significant business area, these institutions must comply with detailed requirements (to be applied considering the institutions' size, complexity, structure and risk profile).

Partially consolidated rules on outsourcing also apply to financial institutions governed by the Federal Act on Financial Institutions, including those not subject to the Outsourcing Circular (ie, asset managers and trustees) and financial services providers governed by the Federal Financial Services Act (ie, client advisers and producers and providers of financial instruments), as well as financial market infrastructures governed by the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (ie, stock exchanges, multilateral trading facilities, central counterparties, central securities depositories, trade repositories and payment systems).

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Disclosure of PI to third parties must follow the general data processing principles. Non-compliance with such principles must be justified. Disclosure of sensitive PI or personality profiles always requires justification (even if it is conducted in compliance with the general principles).

The communication of PI between companies belonging to the same corporate group is deemed to be a disclosure of PI to third parties.

Regularly disclosing information contained in a PI collection entails a registration obligation for such collections.

No specific restrictions apply on the selling of PI or sharing of PI for online targeted advertising purposes, subject to the general rules on unsolicited mass advertising.

Under the revised DPA, data subjects must be informed about the identity or categories of recipients in the case of disclosure to third parties.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

PI may only be transferred outside Switzerland if the privacy of the data subject is not seriously endangered, in particular, due to the absence of legislation that guarantees adequate protection in the jurisdiction where the receiving party resides. The Federal Data Protection and Information Commissioner (FDPIC) has published on its website a list of jurisdictions that provide adequate data protection. The European Economic Area countries and Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, Monaco, New Zealand and Uruguay are generally considered to provide an adequate level of data protection concerning PI of individuals (however, many do not with respect to PI of legal entities), while the laws of all other jurisdictions do not provide adequate data protection.

In the absence of legislation that guarantees adequate protection, PI may only be transferred outside Switzerland if:

- sufficient safeguards, in particular, contractual clauses, ensure an adequate level of protection abroad;
- the data subject has consented in the specific case;

- the processing is directly connected with the conclusion or the performance of a contract and the PI is that of a contractual party;
- disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- disclosure is required in the specific case to protect the life or the physical integrity of the data subject;
- the data subject has made the PI generally accessible and has not expressly prohibited its processing; or
- disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules (ie, binding corporate rules) that ensure an adequate level of protection.

Data transfer agreements or data transfer clauses are regularly used in practice. It is the responsibility of the data transferor to ensure that an agreement is concluded that sufficiently protects the rights of the data subjects. The data transferor is free to decide whether or not to make use of a standard form. The FDPIC must be notified of such safeguards and may, over a period of 30 days, review the safeguards; although, the data transferor does not have to wait for the result of the FDPIC's review or obtain approval. The FDPIC has pre-approved the European Commission's standard contractual clauses (adopted by the Commission Implementing Decision 2021/914 (EU SCC)) as safeguards, which provide adequate data protection, although they must be adapted to also cover PI of legal entities and further requirements arising out of Swiss data protection law. If PI is transferred based on safeguards that have been pre-approved by the FDPIC, the FDPIC only has to be informed about the fact that such safeguards form the basis of the data transfers (and the safeguards themselves do not need to be filed).

Another acceptable method for ensuring adequate data protection abroad are binding corporate rules (BCRs) that sufficiently ensure data protection in cross-border data flows within the same legal person or company or between legal persons or companies that are under the same management. The owner of the data collection must notify the BCRs to the FDPIC. The BCRs should address at a minimum the elements covered by the EU SCC.

The cross-border data transfer regime remains largely unchanged under the revised DPA, however, the Federal Council (and no longer the FDPIC) will determine which jurisdictions provide adequate data protection legislation. Further, the duty to notify the FDPIC in the case cross-border transfer is based on pre-approved standard contractual clauses or BCR is removed. Also, a cross-border transfer may be justified by direct connection to the conclusion or performance of a contract between the controller and a third party in the interest of the data subject (whereas under the current regime, the data subject must be a party to the contract justifying transfer or substituting consent). Consent as a justification has been slightly amended, such that consent must be explicit. As one of the very few rules going beyond the requirements of the GDPR, every jurisdiction to which PI is transferred to and safeguards implemented or exemptions applied, as applicable, must be disclosed to the data subjects (irrespective of whether or not such destination jurisdiction provides for adequate data protection legislation).

Further transfer

33 If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

In the case of service providers, onwards transfer is only permissible under the same conditions as the initial transfer abroad, otherwise, the owner of the data collection in Switzerland may be breaching DPA provisions. Accordingly, when transferring data abroad under a data transfer agreement, this point should be addressed explicitly (as, for example, the EU SCC does).

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No statutory localisation requirements arise from the DPA (or revised DPA). However, special rules as regards localisation may apply in regulated markets. In particular, Circular 2018/03, issued by the Swiss Financial Market Supervisory Authority FINMA (Outsourcing Circular), provides that the data necessary for restructuring or resolving the financial institutions subject to the Outsourcing Circular must at all times be accessible in Switzerland (ie actually be stored or mirrored in Switzerland). Thus, exclusive hosting abroad, even if access at all times is ensured, would not meet this requirement.

RIGHTS OF INDIVIDUALS

Access

35 Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Any data subject may request information from the owner of a data collection as to whether PI concerning him or her is being processed (right of access). If this is the case, the data subject has the right to be informed about:

- all available PI in the data collection concerning the data subject, including available information on the source of the data;
- the purpose and, if applicable, the legal basis of the processing;
- categories of PI processed;
- other parties involved with the data collection; and
- the recipients of the PI.

The owner of a data collection must generally comply with requests by a data subject and provide the requested information in writing within 30 days of the receipt of the request. If it is not possible to provide the information within such time, the owner of the data collection must inform the data subject of the time during which the information will be provided.

Moreover, a request may be refused, restricted or delayed if:

- a formal law so provides;
- it is required to protect the overriding interests of third parties; or
- it is required to protect an overriding interest of the owner of the data collection, provided that the PI is not shared with third parties.

An access request must usually be processed free of charge. As an exception, the owner of the data collection may ask for an appropriate share of the costs incurred if:

- the data subject has already been provided with the requested information in the 12 months before the request and no legitimate interest in the repeated provision of information can be shown, whereby, in particular, a modification of the PI without notice to the data subject constitutes a legitimate interest; or
- the provision of information entails an exceptionally large amount of work.

The share of the costs may not exceed 300 Swiss francs. The data subject must be notified of the share of the costs before the information is provided and may withdraw its request within 10 days.

Other rights

36 | Do individuals have other substantive rights?

The Federal Data Protection Act (DPA) further provides for the following rights for data subjects:

- the right of rectification;
- the right of erasure; and
- the right to object to the processing or disclosure of PI.

Further, if it is impossible to demonstrate whether PI is accurate or inaccurate, the data subject may also request the entry of a suitable remark to be added to the particular piece of information or data.

The revised DPA introduces a general right of data portability (ie, a right to receive own PI in a commonly used electronic format, where the processing is carried out by automated means and based on consent or occurs in direct connection with the conclusion or performance of a contract; and a right to request transfer of such PI to another controller if it does not involve a disproportionate effort).

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Violations of the DPA may be asserted by the data subject in a civil action against the violator. The data subject may file claims for damages and reparation for moral damages or the surrender of profits based on the violation of his or her privacy and may request that the rectification or destruction of the PI or the judgment be notified to third parties or be published.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

In the case of breach, a data subject needs to exercise these rights by itself through civil action. The FDPIC does not have the authority to enforce such individual rights by him or herself.

Under the revised DPA, the FDPIC's enforcement authority is significantly increased and it may, for example, upon request by a data subject, initiate an investigation and, based thereon, render certain binding administrative measures aimed at the processing operations and to restoring compliance with the data protection provisions (eg, adjustment, suspension or termination of processing, destruction or deletion of PI, and granting of access to PI as requested by the data subject). However, it may not award any monetary damages or compensation or impose any fines or other sanctions.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

The most important derogations, exclusions and limitations were mentioned earlier. As previously stated, depending on the subject matter, there may be additional regulations applicable that can have a significant impact on the general data protection rules, adding to them, modifying them or even exempting them from the application.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The use of cookies is generally permissible, provided that the operator of the website (or another online service), which installs the cookie on the user's computer (or another device) informs the user about:

- the use of cookies;
- the purpose of the use; and
- the user's right to refuse cookies.

There is no statutory requirement or judicial practice concerning form, but prevailing opinion considers such information to be sufficient if it is placed on a data protection information page or questions and answers sub-page or similar. The cookie banners or pop-ups, which are often seen on websites of other European countries nowadays, seem to be dispensable, although this has not yet been subject to judicial review.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

Switzerland adopted a full consent opt-in regime concerning unsolicited mass advertisement through telecommunications (eg, email, text, multimedia messaging service, fax or automated telephone calls). Under this law, the sender of an unsolicited electronic mass advertisement must seek the concerned recipient's prior consent to receive such mass advertisement and indicate in the advertisement the sender's correct contact information and a cost- and problem-free method to refuse further advertising. If a supplier collects PI relating to his or her customer in connection with a sales transaction, the supplier may use such data for mass advertisement for similar products or services if the customer has been given the option to refuse such advertisement (opt-out) at the time of sale. The law does not specify for how long the supplier may use such customer data obtained through a sales transaction for mass advertisement. A period of about one year from the time of sale seems adequate.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules on targeted online advertising, other than the general rules on unsolicited mass advertisement; however, under the revised DPA, such analysis and subsequent advertising may under certain circumstances amount to a high-risk profiling, requiring explicit consent by the data subjects concerned (or even a data protection impact assessment).

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

There are no specific rules on the use of sensitive PI for marketing purposes, other than the general rules applicable to the processing of sensitive PI.

Profiling

44 | Are there any rules regarding individual profiling?

Under the revised DPA, high-risk profiling (ie, any form of automated PI processing to use such data to assess certain personal aspects

relating to an individual that involves a high risk to the personality or fundamental rights of the individual, as it pairs data that enables an assessment of essential aspects of the personality of such individual) requires explicit consent by the data subjects concerned.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There are no rules specifically applicable to cloud services. In general, PI must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is stored. Anyone processing PI must ensure its protection against unauthorised access, its availability and its integrity. Further, the use of cloud services constitutes an outsourced processing service if the PI is not encrypted during its storage in the cloud and, in the case the servers of the cloud are located outside Switzerland and the PI is not encrypted during its transfer and storage, an international transfer of PI. Additionally, the Federal Data Protection and Information Commissioner has published on its website a non-binding guide outlining the general risks and data protection requirements of using cloud services.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In September 2020, the Swiss parliament adopted a revision of the Federal Data Protection Act (DPA). The revised DPA largely follows the regime provided by EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) with some reliefs and very limited 'Swiss finishes' (as in rules that go beyond the requirements of the GDPR). The revised DPA should allow Switzerland to uphold its status as a country adequately protecting PI from an EU perspective, thereby allowing for easier transfer of PI from the European Union into Switzerland. It is envisaged that it will enter into force on 1 September 2023. The Federal Council is still in the process of drafting the final revised corresponding ordinance.

In August 2021, the Federal Data Protection and Information Commissioner (FDPIC) recognised the EU standard contractual clauses for the transfer of personal data to third countries (issued pursuant to EU Commission Implementing Decision 2021/914/EU) (EU SCC) as a basis for PI transfers to a country without an adequate level of data protection (from a Swiss law perspective), provided that certain necessary adaptations and amendments (as specified in detail by the FDPIC) are made to the EU SCC to comply with Swiss data protection law requirements. The old EU standard contractual clauses, the Swiss Transborder Data Flow Agreement and the Council of Europe model contract to ensure equivalent protection in the context of cross-border data flows, may no longer be concluded and notified as safeguards for adequate data protection abroad, but (if already concluded and notified before 27 September 2021) may be continued to be used for a transitional period until 31 December 2022.

LENZ & STAEHELIN

Lukas Morscher
lukas.morscher@lenzstaehelin.com

Leo Rusterholz
leo.rusterholz@lenzstaehelin.com

Brandschenkestrasse 24
8027 Zurich
Switzerland
Tel: +41 58 450 80 00
Fax: +41 58 450 80 01
www.lenzstaehelin.com

Taiwan

Yulan Kuo, Jane Wang and Brian Hsiang-Yang Hsieh

Formosa Transnational Attorneys at Law

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Taiwan has one piece of legislation, the Personal Data Protection Act (PDPA), which affords comprehensive protection concerning the use, collection and processing of PI by government agencies and private entities. The PDPA sets forth statutory requirements that must be met by entities for the use, collection and processing of PI. Special protections are imposed upon an entity if the PI used, collected or processed by the entity falls into the category of 'sensitive data', which includes a person's health records, genetic information, sexual history and criminal history. An entity that violates the requirements imposed by the PDPA will be subject to provisions imposing both civil and criminal liability on the entity. The PDPA also gives an administrative agency having proper jurisdiction the authority to impose administrative penalties upon the entity.

The PDPA does not explicitly cite any foreign legislation. However, according to the historical record, the drafters of the PDPA did consider the provisions of EU Directive 95/46/EC (the Data Protection Directive), the Organization for Economic Cooperation and Development Guidelines and the Asia-Pacific Economic Cooperation's privacy framework when drafting the PDPA.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The PDPA does not give any single government agency overriding authority to oversee enforcement of the PDPA. As such, there is no particular government agency in Taiwan that has been actively policing personal data protection practices. The PDPA, however, requires Taiwan's Ministry of Justice (an equivalent to the US Department of Justice), to set forth guiding principles for all other government agencies, central and local, to take into account when enforcing the provisions of the PDPA.

Moreover, in response to the European Union's enforcement of the General Data Protection Regulation (GDPR), Taiwan's National Development Council (NDC), a policy advising agency affiliated to the Executive Yuan (the highest agency of the executive branch), established the Personal Data Protection Office (the Office) on 4 July 2018. One of the main functions of the Office is to coordinate the enforcement of PDPA by different government agencies and to examine the current regulations of the PDPA. The Office was appointed by the Executive Yuan to monitor Taiwan's personal data protection issues and the enforcement of PDPA.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The PDPA does not give any particular government agency overriding authority to enforce the data protection law. However, the PDPA does require the Ministry of Justice to set forth guiding principles.

In response to the EU's enforcement of the GDPR, the Personal Data Protection Office was appointed by the Executive Yuan to monitor Taiwan's personal data protection issues and the enforcement of PDPA.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Any breach of the obligations imposed by the PDPA may result in liabilities, civil and criminal, as well as administrative penalties and orders.

An administrative agency with proper jurisdiction over a breach could impose upon the breaching entity a cease-and-desist order that compels the breaching entity to immediately cease collecting, processing and using the relevant PI. The agency could also order the breaching entity to delete the PI possessed by the breaching entity, or to confiscate or destroy the PI that the breaching entity unlawfully collected. The agency may also publish the facts of such a data breach and the name of the breaching entity and its representative.

Administrative penalties may be a fine imposed on the breaching entity and its representative of between NT$20,000 and NT$500,000.

A natural person responsible for the breach will also face criminal penalties, including imprisonment for up to five years and a fine of up to NT$1 million.

Judicial review of data protection authority orders

5 Can PI owners appeal to the courts against orders of the data protection authority?

Where an order is imposed on a PI owner regarding PI matters by the competent authority and the PI owner disagrees with this order, which may be against the PI owner's interests, it may file an administrative appeal to the administrative appeal committee of the competent authority, requesting that the committee reconsider the order. The PI owner can bring the same matter to the courts if it subsequently fails to receive a favourable decision from the committee.

SCOPE

Exempt sectors and institutions

6 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data Protection Act (PDPA) applies to all sectors and organisations, private and public, and all kinds of activity. At the same time, however, some other individual statutes impose specific data protection for some particular types of PI. For instance, financial institutions operate under stringent obligations to maintain the confidentiality of their clients' financial data. Labour laws also impose on employers' certain obligations to keep their employees' personal data confidential.

Interception of communications and surveillance laws

7 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The PDPA does not specifically address invasions of privacy via interception of communications, electronic marketing or monitoring, and conducting surveillance on individuals. Nevertheless, if the invasion of privacy concerns PI as defined in the PDPA, the PDPA will certainly regulate that activity. Additionally, anyone conducting illegal surveillance will violate Taiwan's Criminal Code or the Communication Security and Surveillance Act. These statutes make unlawful surveillance a crime and impose upon offenders criminal penalties, including imprisonment, detention and fines.

Other laws

8 Are there any further laws or regulations that provide specific data protection rules for related areas?

There are many other laws and regulations specifically applied to various activities and industries that provide specific data protection to individuals. For example, the Human Biobank Management Act mandates special protection for the PI of participants who provide biological specimens. The Enforcement Rules for the Financial Technology Development and Innovative Experimentation Act (the Sandbox Act) provide specific rules to manage and protect PI collected from those participating in experiments. Also, the Employment Service Act stipulates that employers are not allowed to force employees or job seekers to provide unnecessary personal information.

PI formats

9 What categories and types of PI are covered by the law?

The PDPA covers all PI without limitation to specific formats of personal data.

Extraterritoriality

10 Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The PDPA explicitly provides that a Taiwan entity or individual will be subject to the obligations set forth by the PDPA for their use, collection or processing of PI of other Taiwan citizens outside the territory of Taiwan. According to the explanatory decree by the Ministry of Justice of Taiwan, if the use, collection or processing of PI occurs outside the territory of Taiwan, the following requirements must be met before the PDPA becomes applicable: the entity engaging in the collection, processing or use of PI is a government agency or non-government entity 'established in Taiwan'; and the PI subject is a Taiwan citizen.

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Yes, the PDPA covers all processing and use of PI. The PDPA does not distinguish between those who control or own PI and does not impose different duties and obligations.

The definitions of PI collection, processing and use under the PDPA are as follows:

- collection: to collect PI in any form or in any way;
- processing: to record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit PI for the purpose of establishing or using a PI file; and
- use: to use PI in any way other than processing.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

According to the Personal Data Protection Act (PDPA), a non-government entity (including natural persons and private agencies) may collect and process PI for a specific purpose in the following situations:

- the collection or processing of PI is permitted by law;
- the collecting or processing party and the PI subject (individual) form or are going to form a contractual relationship, and the collection and processing of PI is done with proper safety measures;
- the PI is published by the PI subject or is legally published by a third person;
- the collection or processing of the PI is done by a research entity where the collection or processing is necessary to perform statistical or academic research in the public interest and the collecting party or the providing party of such PI has altered the PI such that the subject cannot be identified by the PI;
- the collection or processing is made with the PI subject's consent;
- the collection or processing of the PI is done to enhance the public interest;
- the PI is collected from publicly available resources; and
- the right or interest of the PI subject will not be harmed.

However, where the PI is collected from publicly available resources, the PI shall not be further collected or processed if the data subject objects to such collection.

Also, according to the PDPA, the use of the PI will be permitted if such use is within the specific purpose for collecting and processing the PI.

Moreover, while requesting the PI subject's consent, the collecting party must disclose the following information:

- the name of the authority collecting the PI;
- the purpose of the collection;
- the category of the PI;
- the period, area, object and method of use of the PI; and
- the rights of the data subject to request:
  - a review of his or her PI;
  - to make duplications of his or her PI;
  - to supplement or correct his or her PI;

- to have the collection, processing or use of his or her PI discontinued;
- to have his or her PI deleted from the record; and
- to exercise his or her rights if he or she chooses not to agree to the collection.

However, in the following situations, the above disclosures are not required:

- the exemption from the obligation to disclose is permitted by law;
- the collection of PI is necessary for a government agency to perform its official duties or for a non-government entity to fulfil a legal obligation;
- the disclosure will impede a government agency in performing its official duties;
- the disclosure will impair the public interest;
- the PI subject should have already known the content of the notification; and
- the collection of personal information is for non-profit purposes, and it clearly will not harm the interest of the data subject.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

The PDPA does impose more stringent rules for specific types of PI. Sensitive PI, such as medical records, medical treatment, genetic information, sexual history, health examinations and criminal records can be collected, processed and used only in the following situations:

- the collection, processing and use of PI is permitted by law;
- the collection, processing and use of PI is necessary for a government agency to perform its official duties or for a non-government entity to fulfil a legal obligation, and proper safety measures are taken during and after the collection, processing and use of PI;
- the PI is published by the PI subject (individual) or is legally published by a third person;
- the collection, processing or use of PI is made by a government or research entity for the purpose of enhancing medical treatment or health or to prevent criminal activities, where the collection, processing and use of PI is necessary to perform statistical or academic research, and where the collecting party or the providing party of such PI has altered the PI such that the individual cannot be identified;
- the collection, processing and use of PI is done to assist a government or non-government entity in performing official duties or fulfilling a legal obligation, and proper safety measures are taken during and after the collection, processing and use of PI; and
- to the extent permitted by law, the collection, processing and use of PI is made with the PI subject's written consent.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Yes, under the Personal Data Protection Act (PDPA), if the PI is collected without the consent of the data subject, the PI owner is required to notify the data subject of its possession of his or her PI before the owner processes or uses the PI. The notice must include the following information:

- the source of the collection;
- the name of the authority collecting, processing or using the PI;
- the purpose of the collection;
- the category of the PI;
- the period, area, object and method of use of the PI; and
- the rights of the data subject to request a review of his or her PI, to make duplications of his or her PI, to supplement or correct his or her PI, to have the collection, processing or use of his or her PI discontinued, and to have his or her PI deleted from the record.

Exemptions from transparency obligations

15 | When is notice not required?

In the following situations, notice to the data subject of the use and processing is not required:

- the exemption from the obligation to give notification is permitted by law;
- the collection of the PI is necessary for a government agency to perform its official duties or for a non-government entity to fulfil a legal obligation;
- giving notice will impede a government agency in performing its official duties;
- giving notice will impair the public interest;
- the PI subject should have already known the content of the notification;
- the collection of personal information is for non-profit purposes, and the collection will clearly not harm the interest of the data subject;
- the PI is published by the data subject or is legally published by a third person;
- the PI owner cannot inform the data subject or his or her representative;
- the processing or use of the PI is done by a research entity where it is necessary to perform statistical or academic research in the public interest and the collecting party or the providing party of such PI has altered the PI such that the individual cannot be identified; and
- the PI is collected by the mass media for the purpose of reporting news in the public interest.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

The PDPA does not set forth standards for the quality, currency and accuracy of PI. However, the PDPA requires the PI owner to maintain the accuracy of PI and to actively supplement or correct the PI, or to do so upon request by the data subject. Additionally, if the accuracy of the PI is in dispute, the PI owner must actively cease processing or using the PI or do so upon request by the data subject. However, if the processing or use of the PI is necessary to perform official duties or to fulfil legal obligations, or is consented to by the data subject, the PI owner may continue its processing or use of the PI after recording that the PI is in dispute.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The PDPA does not restrict the volume of PI that may be collected, and the PDPA imposes more stringent rules to restrict the collection, processing and use of the sensitive PI.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The PDPA does not restrict the amount of PI that may be held or the specific length of time it may be held. Nevertheless, the PDPA requires the PI owner to cease processing or using the PI once the specific purpose of the collection, processing or use of the PI no longer exists or the term of such purpose has expired. However, if processing or using the PI is necessary to perform official duties or to fulfil legal obligations, or is consented to by the data subject, the PI owner may continue to process or use the PI.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes, the purposes for which PI can be used are restricted by the PDPA. The PDPA provides a 'purpose limitation principle' under which the rights and interests of data subjects must be respected while the PI owner collects, processes or uses PI, and any collection, processing or use of PI must be conducted in good faith, must not go beyond specific purposes and must be performed in connection with the purpose of the collection.

The PDPA stipulates that when a data subject's PI is collected, the data subject must be expressly informed of the purpose of the collection, and the processing or use of the PI must be performed in connection with the purpose. In addition, there are some exceptions to the purpose limitation principle. The PDPA allows PI to be used for new purposes if any one of the following situations exists:

- using PI for a new purpose is permitted by law;
- using PI for a new purpose is done to enhance a public interest;
- using PI for a new purpose is to prevent harm to the life, body, freedom or property of the data subject (individual);
- using PI for a new purpose is to prevent harm to the rights and interests of other people;
- PI is used by a research entity or government agency where using the PI for a new purpose is necessary to perform statistical or academic research to advance the public interest, and the collecting party or the providing party of such PI has altered the PI so that the individual cannot be identified;
- using PI for a new purpose is agreed to by the data subject; and
- using PI for a new purpose will benefit the rights of the data subject.

However, none of these exemptions applies to any sensitive data.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

No. Currently, the PDPA does not provide any provisions regarding automated decision-making.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

A government agency or non-government entity keeping possession of any PI privacy by design must adopt appropriate cybersecurity measures to prevent the PI from being stolen, altered, damaged, destroyed or disclosed. If the PI owner is a government agency, it is required to assign specific persons to be in charge of the security of PI. Also, the Personal Data Protection Act (PDPA) Enforcement Rules provide guidelines for such security measures. For example, the PI owner may assign and allocate personnel to manage PI, establish a mechanism to evaluate risk, prevent leaks, deal with any accidental incidents, establish internal rules, hold educational training and maintain the security system for regular periods. Moreover, the central government may require non-government entities to stipulate internal principles to protect the safety of PI, including how PI will be disposed of after the termination of the relevant business.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The PDPA requires PI owners to notify data subjects of any data breaches if a breach results in PI being stolen, altered, damaged, destroyed or disclosed. Also, some relevant PI regulations specifically applied to particular industries require PI owners to report data breaches to the relevant government authorities. For example, PI owners in the banking and insurance industries are required by the regulations made by the Financial Supervisory Commission to report data breaches to the Commission.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

A government agency or non-government entity must adopt appropriate security and maintenance measures, including, without limitation, establishing internal rules and preserving use records and relevant evidence. In particular, some specific non-government entities, including in the banking and medical sectors, must conduct much stricter obligations requested by relevant PI regulations to strengthen internal data control.

The PDPA stipulates that the relevant government authorities may inspect compliance with the security control measures, the guidelines on disposing personal data upon business termination and the restrictions on cross-border transfers, and may conduct any other routine inspections when they deem necessary to suspect any possible violation. They may also order relevant personnel of the non-government agencies to provide necessary explanations or supporting documents.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Under the Personal Data Protection Act (PDPA), a government agency keeping possession of PI is required to appoint a data protection officer (DPO), but this does not apply to a non-government entity. The responsibility of the DPO is to prevent PI from being stolen, altered, damaged, destroyed or disclosed. However, the guidelines for security measures afforded by the PDPA Enforcement Rules suggest

that a non-government entity appoint a DPO to manage the PI that it possesses. Also, some relevant PI regulations specifically applied to particular industries require PI owners to appoint a DPO. For example, the regulations respectively applicable to banks, insurance providers, short-term educational centres and medical sectors require entities in these industries to appoint a DPO.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The PDPA does not require PI owners or processors to maintain internal records of their processing or use of PI. However, the PDPA Enforcement Rules suggest that PI owners or processors, whether government or non-government entities, keep internal records to protect the security of PI. On the other hand, some relevant PI regulations specifically applicable to particular industries require PI owners or processors to maintain internal records of the use of PI. For example, the regulations made by the Financial Supervisory Commission require PI owners in the banking and insurance industries to maintain such internal records.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The PDPA does not address risk assessments for privacy impacts. However, the PDPA Enforcement Rules suggest that PI owners or processors, whether government or non-government entities, establish a mechanism to assess the risk of collecting, processing and using PI. Some relevant PI regulations specifically applied to particular industries further require PI owners or processors to periodically conduct risk assessments on their collection, processing or use of PI. For example, online shops and platforms, banks and insurance providers, real estate agencies, and short-term educational centres are obliged to conduct such PI risk assessments. Notwithstanding the foregoing, these regulations and rules do not provide clear definitions or substantial requirements for conducting risk assessments in practice.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Currently, there is no provision of the PDPA and its relevant regulations specifically regulating the privacy-by-design or privacy-by-default approaches.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

PI owners or processors are not required to register with the supervising authority before carrying out the collection, processing or use of PI.

Other transparency duties

29 | Are there any other public transparency duties?

Under the Personal Data Protection Act, a government agency is required to publish the following information on the internet or by other proper means for review:

- the name of a PI file;
- the name of the government entity keeping the PI file and its contact information;
- the legal basis for and purpose of keeping the PI; and
- the classification of PI.

Non-government entities keeping PI are not obliged to make such publication.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

There is no provision of the Personal Data Protection Act (PDPA) specifically regulating the transfer of PI to entities that provide outsourced processing services. However, because the transfer of PI is categorised as an activity of processing or using PI under the PDPA, the transfer of PI to entities that provide outsourced processing services must comply with all provisions regulating the processing or use of PI. As such, while transferring PI to another entity, the PI owner is obliged to prevent the PI from being stolen, altered, damaged, destroyed or disclosed.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Disclosing PI to other recipients, whether based on selling PI or sharing for targeted advertising purposes, must all be done under the regulations for the use of PI under the PDPA. That is, for a non-government entity, if disclosing PI to other recipients is within the scope of a specific purpose for collecting and processing the PI, the PI owner may freely make such disclosure. Otherwise, the disclosure can be made only if it satisfies the requirements under which the use of PI for new purposes is allowed. However, the recipient must notify the data subject of its possession of PI before processing or using the PI. For the requirements of using PI for new purposes and contents of notification given by the recipients and their exceptions.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The PDPA does not impose restrictions on international transfers of PI by government entities, but non-government entities are restricted by the central government from transferring PI outside the jurisdiction if any one of the following situations occurs:

- the transfer involves significant national interests, such as national security, diplomatic or military secrets;
- a national treaty or agreement specifies other requirements on transfers;
- the country where the PI will be received lacks proper regulations on the protection of PI and the transfer might harm the rights and interests of data subjects; or
- the international transfer of PI is made to evade the provisions of the PDPA.

For example, the Taiwan National Communications Commission has issued an order to forbid the communications enterprises to transfer their users' personal data to mainland China. In 2022, the Ministry of Health and Welfare also issued an order to forbid the social worker's office to transfer PI to mainland China.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restriction on cross-border transfers applies to all non-government entities without differentiation between service providers or PI owners.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

While the PDPA itself does not specifically require data localisation, regulations relating to financial institutions do. For example, under the 'Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation', the PI outsourced to a cloud service provider must be processed and stored within the territories of Taiwan in principle. If the PI is processed and stored outside Taiwan, the following rules shall be applied:

- the financial institution shall retain rights to designate the location for the processing and storage of the data;
- the data protection regulations in such jurisdiction must not be lower than the requirements of the Taiwan; and
- except with the approval of the competent authority, copies of PI must be retained in Taiwan.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, the Personal Data Protection Act (PDPA) gives data subjects the right to access their personal information held by PI owners. Data subjects may request PI owners to allow a review of their PI or to provide duplications of their PI. However, in any one of the following situations, the above requests may be declined:

- the request might interfere with or harm national security, diplomatic or military secrets, economic interests or other significant national interests;
- the request might interfere with the performance of official duties; or
- the request might negatively affect the interests of the PI owner or a third person.

Other rights

36 | Do individuals have other substantive rights?

In addition to the data subject's right to request PI owners to allow a review of his or her PI or to provide duplications of his or her PI, the PDPA provides data subjects with the right to have his or her data corrected, to cease the collection, processing or use of his or her PI, and to delete his or her PI. These rights of data subjects cannot be waived by data subjects or be limited contractually in advance.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes. Data subjects are entitled to monetary damages if their PI is breached, as follows:

- Compensation is not limited to loss of costs, as non-pecuniary damages such as emotional distress and loss of reputation are available. If the reputation of the PI subject is harmed owing to the PI owner's breach of the PDPA, the PI subject may request the court to order the PI owner to restore his or her reputation.
- If the data subject has difficulty establishing the actual damages caused by the breach, he or she may request the court to grant compensation of an amount of no less than NT$500 but no more than NT$20,000 for each breach.
- If the breach causes damages to multiple data subjects by the same cause and fact, those victims are entitled to monetary compensation of no more than NT$200 million. However, if the value of the interests the breaching party may gain from the alleged violation is higher than NT$200 million, the victims are entitled to monetary compensation of no more than the established value of said interests.
- If the damages to multiple data subjects by the same cause and fact exceed NT$200 million, the limitation on compensation granted of the amount of no less than NT$500, as provided under the condition specified in the second bullet point above, shall not apply.
- Statute of limitation: the right to claim compensation will be blocked after two years from the date on which the data subject became aware of the damages and of the person who is liable for the damages, or five years from the date of the occurrence of the damage.

If the breaching entity is a non-government entity, the entity may be free from liability if the entity successfully shows that the breach occurred without intent or negligence.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Data subjects seeking monetary damages or compensation must do so by filing a lawsuit at a court with proper jurisdiction.

Data subjects seeking remedies other than monetary damages or compensation where the PI owner is a non-government entity may go to the courts or report the matter to a government agency having proper jurisdiction.

If the PI owner is a government agency, data subjects must file an administrative appeal against this government agency and, if not successful, then file an administrative lawsuit.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

The Personal Data Protection Act will not apply where the collection, processing and use of personal information by a person is merely for personal and family activity, as well as where audiovisual information is collected, processed or used in public places or public activities without association to other personal information (eg, video recorded by dashboard cameras).

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

The Personal Data Protection Act (PDPA) does not contain specific provisions to regulate the use of cookies. However, if the information collected through cookies matches the definition of PI, the PDPA shall apply. Taking distributing targeted advertisements, for example:

- when the server collects PI from an individual, it must comply with the rules regulating PI collection under the PDPA;
- when the server analyses the PI collected, it must comply with the rules regulating PI processing and use under the PDPA; and
- when the server uses its analysing report to distribute targeted advertisements, it must comply with the rules regulating PI use under the PDPA.

In this regard, more and more websites utilise a pop-up window seeking users' consent to the collection, processing and use of their PI when the user visits the website for the first time.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

Under the PDPA, when a non-government entity uses the PI collected to do marketing, regardless of whether it is via email, fax, telephone or other electronic forms, it must stop if the data subject so requires. Also, when PI is first used by a non-government entity for marketing, the data subject must be advised of the measures for declining such marketing use. The expense for carrying out these measures must be borne by that entity.

Targeted advertising

42 | Are there any rules on targeted online advertising?

The PDPA and its related regulations do not provide specific provisions for targeted advertising. However, the advertising provider must comply with the general rules under the PDPA when collecting, processing and using the PI.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Yes. Sensitive PI can only be collected, processed and used in the following situations:

- the collection, processing and use of PI is permitted by law;
- the collection, processing and use of PI is necessary for a government agency to perform its official duties or for a non-government entity to fulfil a legal obligation, and proper safety measures are taken during and after the collection, processing and use of PI;
- the PI is published by the PI subject (individual) or is legally published by a third person;
- the collection, processing or use of PI is made by a government or research entity for the purpose of enhancing medical treatment or health or to prevent criminal activities, where the collection, processing and use of PI is necessary to perform statistical or academic research, and where the collecting party or the providing party of such PI has altered the PI such that the individual cannot be identified;
- the collection, processing and use of PI is done to assist a government or non-government entity in performing official duties or fulfilling a legal obligation, and proper safety measures are taken during and after the collection, processing and use of PI; and
- to the extent permitted by law, the collection, processing and use of PI is made with the PI subject's written consent.

萬國法律事務所
SINCE 1974 Formosa Transnational Attorneys at Law

Yulan Kuo
yulan.kuo@taiwanlaw.com

Jane Wang
jane.wang@taiwanlaw.com

Brian Hsiang-Yang Hsieh
brian.hsieh@taiwanlaw.com

13F
136 Section 3
Jen Ai Road
Taipei City 106
Taiwan
Tel: +886 2 2755 7366
Fax: +886 2 2755 6486
www.taiwanlaw.com

Profiling

44 | Are there any rules regarding individual profiling?

No. Currently, the PDPA does not specify any rules regarding individual profiling.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There are no specific rules or regulatory guidance on the use of cloud computing services under the PDPA. The use of cloud computing services must comply with all rules regulating the collection, processing and use of PI under the PDPA. Cloud services might trigger the following two issues under the PDPA:

- A cloud service provider and its corporate client maintain a contractual relationship with each other. As such, under the PDPA, the corporate client will be responsible for the cloud service provider's violation of the PDPA. Also, the corporate client is required to supervise the works of the cloud service provider with reasonable efforts, such as establishing a limited scope, classification, specific purpose and period for collecting, processing or using personal information, and keeping records of the works engaged in by the cloud service provider. The cloud service provider, on the other hand, must notify the corporate client if it believes that the client's instructions violate the PDPA.
- Cloud services often involve cross-border data transmissions. The cross-border data transmissions must comply with the specific requirements under the regulations governing the outsourcing of financial institution operations. For example, PI outsourced to

a cloud service provider must be processed and stored within the territories of Taiwan in principle. If the PI is processed and stored outside Taiwan, the following rules shall be applied:

- the financial institution shall retain rights to designate the location for the processing and storage of the data;
- the data protection regulations in such jurisdiction must not be lower than the requirements of the Taiwan; and
- except with the approval of the competent authority, copies of PI must be retained in Taiwan.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The EU General Data Protection Regulation (GDPR), effective since 25 May 2018, has made a great impact upon many Taiwanese entities doing business with EU residents and entities. In response, Taiwan's National Development Council (NDC), a policy-advising agency affiliated to the Executive Yuan (the highest agency of the executive branch), established the Personal Data Protection Office (the Office) on 4 July 2018. According to the NDC, the main functions of the Office include consulting with the European Commission on obtaining its recognition for an adequate level of protection as set out in article 45 of the GDPR, and to be a platform coordinating the enforcement of the Personal Data Protection Act (PDPA) by different government agencies and to examine the current regulations of the PDPA. The Office was appointed by the Executive Yuan to monitor Taiwan's personal data protection issues and the enforcement of the PDPA.

To receive adequate recognition from the European Commission, the Office completed its national evaluation report at the end of 2018. This report was filed to the European Commission's Directorate-General for Justice and Consumers (DG JUST). In early March 2019, the then-head of DG JUST, Tiina Astola, expressed the European Commission's gratitude to Taiwan for its effort in working together with the European Union to improve personal data protection policy. Although the report is still under review by the European Commission, the NDC announced that it would keep discussing this issue with the European Commission and adjust the PDPA if needed based on its continued communications with the European Commission and the development of domestic industries. To date, the Office finished its first run of discussions with the European Commission. The European Commission's reviewing process is ongoing; the Office will work closely with the European Commission to adjust Taiwan's PDPA and the related regulations, if necessary.

Thailand

John P Formichella, Naytiwut Jamallsawat and Onnicha Khongthon

Formichella & Sritawat Attorneys at Law

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Thailand has a dedicated data protection law; the Personal Data Protection Act BE 2562 (2019) (PDPA) was published on 27 May 2019 in the Royal Thai Government Gazette.

The PDPA aims to secure individual and personal data protection and impose obligations on businesses when collecting, using and disclosing personal data. However, based on the Royal Decree on Organisations and Businesses, under which personal data controllers are exempt from their obligations under Personal Data Protection Act Nos. 1 and 2 (the Royal Decree), the enforcement date was postponed to 1 June 2022. The Royal Decree lists various types of business that are qualified for the above exemption, including enterprises in communication, telecommunication, digital, science, technology, banking, education, industrial and commercial industries, among others.

The PDPA is based mainly on the EU General Data Protection Regulation (GDPR), and therefore, there are several similarities between the two. For example, both texts have similar provisions regarding the legal basis of processing, as both list consent, the performance of a contract, legal obligations, legitimate interest or vital interest as a legal basis.

In addition, the PDPA mirrors the GDPR's extraterritorial applicability and applies to data controllers and data processors outside of Thailand if they process the personal data of data subjects in Thailand and offer goods and services to, or monitor the behaviour of, the data subjects. Moreover, both texts empower data subjects with several rights, including the right to erasure, the right to be informed, the right to object, data portability and access.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The authority responsible for overseeing and enforcing data protection law in Thailand is the Personal Data Protection Committee (PDPC). The PDPC has the following duties and powers:

- to make the master plan on the operation for the promotion and protection of personal data, which is consistent with policies, national strategies and relevant national plans, to propose to the committee of the national digital economy and society, per the law governing the development of the digital economy and society;
- to promote and support government agencies and the private sector in carrying out activities per the master plan under the above clause, as well as to conduct the evaluation of the operation result of such master plan;
- to determine measures or guidelines of the operation concerning personal data protection to comply with the PDPA;
- to issue notifications or rules for the execution of the PDPA;
- to announce and establish criteria for protecting personal data that is sent or transferred to a foreign country;
- to announce and develop guidelines for the protection of personal data as guidelines with which the data controller and the data processor shall comply;
- to recommend the Cabinet on the enactment, or revision, of the existing laws or rules applicable to the protection of personal data;
- to advise the Cabinet on the promulgation of the Royal Decree or reconsideration of the suitability of the PDPA at least every five years;
- to provide advice or consultancy on any operation for the protection of personal data of the government agency and private agency, in acting in compliance with the PDPA;
- to interpret and render rulings concerning the issues arising from the enforcement of the PDPA;
- to promote and support learning skills and understanding on the protection of personal data among the public;
- to encourage and support research for the development of technology relating to the protection of personal data; and
- to perform any other acts as prescribed by the PDPA, or other laws, which state the duties and power of the PDPC.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Currently, there are no legal obligations on the data protection authority to cooperate with other data protection authorities.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection law lead to civil, criminal and administrative liability penalties as follows:

Civil liability penalties

Under the PDPA, a data controller or data processor, whose operations violate personal data protection, or fail to comply with the provisions of the PDPA, shall compensate the data subject for these damages,

whether such violations are intentional or negligent, except where the data controller or the data processor can prove that such violations are a result of:

- a force majeure, or the data subject's act or omission to act; or
- action taken in compliance with an order of a government official exercising its duties and power by law.

The compensation under the above-mentioned includes all necessary expenses incurred by the data subject to prevent the damages likely to occur or that were spent to suppress the injuries that occurred.

Criminal liability penalties

Under the PDPA, the maximum penalty for non-compliance under sections 26–28 is a fine not exceeding 5 million baht issued by the expert committee.

Depending on the violation that has occurred under sections 26–28 of the PDPA, the penalty may also be imprisonment for a term not exceeding one year.

Administrative liability

Under the PDPA, the data controller or the data processor who violates the law could face administrative fines of up to 5 million baht.

In addition, the Notification of the Personal Data Protection Committee regarding guidelines on the administrative penalties of the expert committee prescribes the classification of violations in two levels:

- Non-severe level: those PI owners or PI processors who violate the PDPA at this level will be penalised with a warning or an order to cease any unlawful action within a stipulated time.
- Severe level: those PI owners or PI processors who did not conform with the orders of an expert committee or violate the PDPA at this level will be penalised with an administrative fine as specified under the PDPA.

There is no definition under the above Notification on the severity levels of the violation. The determination of the severity must be made by the expert committee based mainly on the result and impact of the violation in this regard.

1.5 Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Under the PDPA, orders of the data protection authority are deemed finalised after issuing. However, as per the Act on Establishment of Administrative Courts and Administrative Court Procedure BE 1999, it is prescribed that orders made by unlawful acts of authorities can be appealed under the jurisdiction of the Administrative Court. Therefore, the owner has the rights to appeal orders from data protection authorities to the Administrative Court if such orders were made by unlawfully.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data Protection Act BE 2562 (2019) (PDPA) shall exclude its application to the following organisations and activities:

- the PDPA does not apply to the operation of public authorities having the duties to maintain state security, including financial security of the state or public safety, including the responsibilities concerning the prevention and suppression of money laundering, forensic science or cybersecurity, trial and adjudication of courts and work operations of officers in legal proceedings, legal execution and deposit of property, including work operations per criminal justice procedures;
- the PDPA does not apply to the Thai parliament, including the Personal Data Protection Committee appointed by parliament, which collects, uses or discloses personal data in their consideration under the duties;
- the PDPA further excludes the operation of data undertaken by a credit bureau company and its members, according to the law governing the functions of a credit bureau business; and
- the PDPA provides for certain processing circumstances, including for a person or a juristic person who uses or discloses personal data collected only for the activities of mass media, fine arts or literature that are only per professional ethics or for the public interest.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The PDPA covers the interception of communications, electronic marketing, and the monitoring and surveillance of individuals.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

The Credit Information Business Act BE 2545 (2002) (CIBA) provides specific data protection rules for credit information or facts about customers applying for credit. To provide credit information to a financial institution member of a credit information company (member) or a user who is a member or a legal entity that conducts credit business as part of its regular business.

Under CIBA, only credit information companies can operate credit information businesses. CIBA prohibits credit information companies, data controllers and data processors running in Thailand to use, control or process data outside Thailand and does not store information. CIBA also prohibits the processing of data older than the specified age. The undertaking of a credit information business can only be done after receiving approval from the Minister of Finance to establish a limited company or a public limited company and obtaining a licence from the Minister.

PI formats

9 | What categories and types of PI are covered by the law?

All PI, whether in any format (writing, electronic or photo, etc), are covered by the PDPA. In addition, the PDPA defines 'personal data' as any information relating to a person that enables the identification of such person, whether directly or indirectly; however, this does not include the information of deceased persons.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The PDPA applies to the collection, use or disclosure of the PI of data subjects in Thailand regardless of whether the collection, use or disclosure of PI takes place in Thailand or not.

Concerning extraterritorial scope, the PDPA applies to PI owners and PI processors outside Thailand whose collection, use or disclosure of PI concerns data subjects in Thailand. Extraterritorial coverage

applies to activities related to offering goods or services to data subjects in Thailand, regardless of whether payment is required or where the data subjects' behaviour is monitored in Thailand.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

There is a distinction between those who control or own PI and those who provide PI processing services to owners. The owner and controller of PI are regarded as data controllers under the PDPA. A data controller is a natural person or juristic person who has the power and duties to make decisions regarding the collection, use or disclosure of PI.

Further, a processor of PI is regarded as a data processor under the PDPA. A data processor is a person (or juristic person) who operates by collecting, using or disclosing the PI under the order given or on behalf of a data controller.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Personal Data Protection Act BE 2562 (2019) (PDPA) states that PI owners (controllers) shall not collect, use or disclose the PI unless the data subject has provided:

- prior consent;
- when processing is necessary for the performance of a contract;
- why processing is necessary for compliance with a law to which the PI owner is subjected;
- for suppressing danger to a data subject's life;
- for the performance of a task carried out in the public interest by the PI owner the achievement of the purpose relating to public interest research and statistics; or
- for the legitimate interest of the PI owner where such interest does not override those of the data subject.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Section 26 of the PDPA requires explicit consent for the collection of PI on racial, ethnic origin, political opinion, cultural, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic information, biometric data or any data that may affect the data subject in the same manner (sensitive data). In addition, supplemental regulations regarding sensitive data will be issued by the Personal Data Protection Committee and may further specify more requirements relating to the processing of sensitive data.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The Personal Data Protection Act BE 2562 (2019) (PDPA) requires a PI owner to provide data subjects with information relating to PI processing either before or at the time of the PI collection.

The PDPA states that information provided to a data subject must include:

- details of the PI to be collected, used or disclosed;
- purposes of collection for use or disclosure of the PI, including the legal basis for the collection;
- data subject rights (the right to erasure, right to object and right of withdrawal, etc);
- the data retention period;
- categories or entities, either as an individual or organisation, who will receive PI; and
- contact details of the PI owner or its representative and the data protection officer (DPO).

In addition, data subjects must be informed of the purpose of processing in an easily accessible form with clear and plain language, which can be in writing or electronic format, to obtain the data subject's consent. The Personal Data Protection Committee may further prescribe a specific or standard form.

Exemptions from transparency obligations

15 | When is notice not required?

The PDPA states that the PI owner must provide information relating to the processing of the PI to the data subject, except when the data subject has already noticed such information.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

The PDPA does not directly impose the standard concerning the quality, currency and accuracy of PI. However, the PDPA requires that the PI owner use all necessary means to ensure that the PI remains accurate, up to date, complete and not misleading. The PDPA also provides that collection of PI is limited to the extent necessary concerning the lawful purpose of the PI owner.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The law does not restrict the types or volume of PI that may be collected.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The PDPA does not restrict the amount of PI that, and the length of time that PI, may be held. In addition, when collecting PI, the PI owner needs to inform the data subject before or during collection that there is the retention of personal data. If it is not possible to specify a fixed retention period, the estimated retention period must be provided.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Under section 21 of the PDPA, the collection, use or disclosure of PI may not be done in a manner that is different from the stated purpose, unless the data subject has been informed of the new purpose and consent has been obtained before or at the time of collection, use or disclosure.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Under the current PDPA, there is no clarification or restriction on automated decision-making. Nonetheless, it is our opinion that automated decision-making must be compliant with the current PDPA regarding collection, use and disclosure of PI.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Personal Data Protection Act BE 2562 (2019) (PDPA) states that a PI owner (controller) and PI processor must provide appropriate security measures (with minimum standards as prescribed by the Personal Data Protection Committee (PDPC)) to prevent the loss, access, use, change, revision, or disclosure of the PI without authorisation. Currently, the PDPA does not provide a list of appropriate technical and organisational measures. Instead, it is further elaborated in the Notification of the Personal Data Protection Committee regarding the security standard of the data controller that the security measures to retain confidentiality, integrity and availability of PI must be applied via physical and electronic means to prevent losses and unauthorised access, usage, modification, rectification and disclosure of PI.

Such security measures must include, at least, the following;

- the control of access to PI and IT (ie, identity proofing and authentication);
- user access management (ie, user registration and user deregistration, user access provisioning, management of privileged access rights, management of the secret authentication information of users, reviews of user access rights and removal or the adjustment of access rights);
- user responsibilities;
- audit trails; and
- privacy and security awareness.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

In the case of a PI breach, the PI owner must notify the PDPC of the breach, except where the personal breach is unlikely to result in a risk to individuals' rights and freedoms.

Under the PDPA, the PDPC must be notified of a PI breach without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. In addition, if a PI breach is likely to result in a high risk to data subjects' rights and freedoms, the PI owner must notify the breach to data subjects. Currently, the PDPA does not provide any exemptions to the requirement that the PI owner must notify data subjects of serious PI breaches. However, specific exemptions will be forthcoming via supplemental regulations from the PDPC.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

As per Thailand's current data protection laws, it is not stated explicitly that owners or processors of PI are required to implement internal controls. However, the owners and the processors are certainly responsible for adopting suitable security measures to prevent data breaches under the Personal Data Protection Act BE 2562 (2019) (PDPA).

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

A data protection officer (DPO) appointment is mandatory in Thailand under certain circumstances. Under the PDPA, a PI owner and PI processor, including their representatives, must appoint a DPO under the following general circumstances:

- the processing is carried out by a public authority or body;
- the activities of a PI owner or PI processor relating to the collection, use or disclosure require regular monitoring of the PI or the system on a large scale; or
- the core activities of the PI owner or the PI processor relate directly to the collection, use or disclosure of specific categories of data (eg, sensitive data, trade union information, personally identifiable information, or any data that may affect the data subject in the same manner as prescribed by the Personal Data Protection Committee (PDPC)).

If a PI owner and PI processor are members of the same business, an appointment of a single DPO is permitted, provided that the data protection officer is easily accessible by both the PI owner and the PI processor. In addition, the appointment of a single DPO is also permitted for public authorities or bodies (which are PI owners or PI processors) that have a large organisational structure or several establishments.

The scope of the DPO's duties are as follows:

- to inform and advise the PI owner, PI processors and their employees on obligations under the PDPA;
- to monitor the performance of the PI owner or PI processor, including their employees or service providers, with processing operations of the PI owner, PI processor and their employees; and
- to act as a contact point for the PI owner and PI processor.

In addition, the appointment must consider the position of a DPO based on expert knowledge and expertise in personal data protection, which the PDPC may further specify.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

An owner and processor of the PI must maintain a record of their PI processing activities (both in writing and electronic form). The PDPA prescribes the specific information that the PI owner must record for the verification of a data subject and the competent authority, which includes:

- the information of the PI owner;
- the purposes of the processing;
- the details of collected PI;
- the rights and means to access the data subjects' PI, including conditions of access and persons authorised to access such PI;
- the retention period of the PI; and
- a general description of security measures.

If a PI owner is a foreign entity, such entity is required to designate a local representative in Thailand. The local representative of the PI owner is obliged to perform activities on behalf of the PI owner, including recording their processing activities in the same manner as the PI owner.

However, the requirements around data processing records shall not apply to a small organisation unless the processing:

- is likely to result in a risk to the rights and freedoms of a data subject;
- is not occasional; or
- includes special categories of sensitive data.

Moreover, the Notification of the Personal Data Protection Committee regarding exempted records of activities of the data controller that is a small organisation has prescribed that the attribution of 'PI owner' may only be ascribed to small organisations that have obtained the exemptions mentioned above and are:

- small or a medium-sized organisations according to laws on the promotion of small and medium-sized organisations;
- community-based organisations or a network of a community-based organisations according to laws on the promotion of community-based organisations;
- community-based cooperatives or a group of farmers according to laws on cooperatives;
- foundations, associations, religious groups or other non-profit organisations; or
- household entities or other organisations that shares the same attribution.

However, the aforementioned attributions do not apply to a small organisation that is a service provider that maintains computer traffic data. Unless such an organisation is an internet cafe.

As for PI processors, the Notification of the Personal Data Protection Committee regarding guidelines to maintain records of processing activities for data processors, which will be effective in December 2022, prescribes that specific information pertaining to the details of the records of processing activities must include at least the following:

- the name and information of PI processors and their representatives (if any);
- the name and information of the PI owner and their representative (if any) who provides instruction to the processors;
- the name and information of the DPO (ie, the venue and method of contact) if a DPO is appointed;
- the types and attributions of collection, usage and disclosure of PI; and
- independents or entities who receive PI, if PI has been transferred to an international jurisdiction.

In addition, PI processors must maintain the records of processing activities at least in writing or electronic form.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Under the PDPA, owners and processors of PI, who have responsibilities to adopt suitable measures, are required to carry out risk assessments in the following circumstances:

- when it is deemed necessary; and
- when there is a change in technology.

As per personal data protection laws, owners or the processors of PI are not required to carry out risk assessments. However, the owners of PI are required to provide impact assessments on the security measures adopted to maintain security and safety standards when deemed necessary by the PDPC or there is a change in the technology of the security measures.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

There is no specific obligation in relation to how PI processing systems must be designed under current personal data protection laws.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

At the current stage of the Personal Data Protection Act BE 2562 (2019) (PDPA), registration with the supervisory authority of PI owners and processors is not required in Thailand. An individual or entity will automatically become a PI owner when it collects the personal data of a data subject. In addition, the PDPA states that the PI owner shall not collect, use or disclose personal data unless:

- the data subject has provided prior consent;
- when processing is necessary for the performance of a contract;
- it is necessary for complying with a law that the PI owner is subject to;
- it is for suppressing danger to a data subject's life;
- it is for the performance of a task carried out in the public interest by the data controller for the achievement of a purpose relating to public interest research and statistics; or
- it is for the legitimate interest of the PI owner where such interest does not override those of the data subject.

Other transparency duties

29 | Are there any other public transparency duties?

No, there are not.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Regarding transfers of PI inside Thailand, the Personal Data Protection Act BE 2562 (2019) (PDPA) prohibits a PI owner from the collection, use or disclosure, including transfer, of PI to third parties, unless the data subject has provided prior consent, or there is a legal basis allowing a PI owner to collect, use or disclose without a data subject's consent (eg, it is for a public interest, legitimate interest or suppressing danger to a data subject's life).

Regarding cross-border transfers, such a transfer will only be permitted to destination countries or international organisations that have an adequate level of protection as prescribed by the Personal Data Protection Committee (PDPC) unless such transfer fulfils the following legal criteria:

- where the consent of the data subject has been obtained;
- it is necessary to perform any obligation under a contract or the transfer is at the request of a data subject;
- it is performed for the significant public interest;
- the transfer is according to the law; and
- where it is to prevent or suppress danger to the data subject or another person's life, body or health when the data subject is incapable of giving their consent.

In addition, the PI owner or PI processor is permitted to transfer the PI abroad only in a case where there are appropriate safeguards in place with effective legal remedies that ensure the data subject's rights as further prescribed by the PDPC.

In the absence of an adequate level of protection, a transfer is permitted when the PI is transferred to affiliates of a national PI owner or PI processor that apply the PI protection policy approved by the PDPC. However, the PDPA has not yet established criteria for PI protection policy, nor has it established the scope of affiliates to implement the above requirement.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Other than the general requirements under the PDPA (eg, rules of consent and legitimate interest), there are no specific restrictions on the sharing (including for the online targeted advertising purposes) and selling of the PI with third parties.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

A cross-border transfer is permitted only to destination countries or international organisations that have an adequate level of protection as prescribed by the PDPC unless such transfer fulfils the following legal criteria:

- the consent of the data subject has been obtained;
- it is necessary to perform any obligation under a contract or the transfer is at the request of a data subject;
- it is performed for the significant public interest;
- the transfer is according to the law; and
- where it is to prevent or suppress a danger to the data subject or another person's life, body or health when the data subject is incapable of giving their consent.

In addition, the PI owner or PI processor is permitted to transfer the PI abroad only in a case where there are appropriate safeguards in place with effective legal remedies that ensure the data subject's rights as further prescribed by the PDPC.

In the absence of an adequate level of protection, a transfer is permitted when the PI is transferred to affiliates of a national PI owner or PI processor that apply the PI protection policy approved by the PDPC. However, the PDPA has not yet established the PI protection policy criteria, nor has it set the scope of affiliates to implement the above requirement.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes, the requirements shall equally apply.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

Under the PDPA, it is not prescribed directly that PI or a copy of PI must be retained within Thailand if PI is transferred or accessed from outside Thailand. However, PI controllers and processors are obliged to adopt security measures that aim to prevent the loss of PI, and retaining a copy of the PI may be one of the prevention measures.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Personal Data Protection Act BE 2562 (2019) (PDPA), data subjects have the right to request access to their personal information held by PI owners. In addition, under the PDPA, the right to access the PI and request a copy of such PI must not adversely affect the rights or freedoms of others.

Regarding the request for access, a data controller must respond to the request without undue delay, but within a maximum of 30 days upon the receipt of the request with no extension period. However, the notification from the relevant authority relating to the exercise of rights, including the cost of implementation, may be published further by the Personal Data Protection Committee (PDPC).

However, a data controller may refuse a request to access the PI, including obtaining a copy or source of the PI, only in the case where the refusal complies with law or court order.

Other rights

36 | Do individuals have other substantive rights?

Under the PDPA, each data subject has the right:

- to erasure: a data subject has the right to request for their PI to be deleted unless exceptions apply;
- to be informed: a data subject has the right to be informed of specific information relating to the collection and processing of their PI;
- to object: a data subject has the right to object to the processing of PI and withdraw his or her consent to the processing at any time;

- to access: a data subject has the right to access PI collected and processed by a PI owner; and
- to data portability: data subjects have the right to receive their PI in a structured, commonly used and machine-readable format as well as to transmit such data to third parties.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Data subjects are provided with the right to claim damages or compensation from a PI owner or PI processor who violates the PDPA, either intentionally or through negligence. In addition, a data subject can lodge a complaint relating to personal data protection to the PDPC. Scope of damages or compensation is provided under the PDPA, which includes any expense a data subject has incurred to prevent injuries likely to be incurred.

In addition, the PDPA provides the authority for a competent court to increase the amount of compensation up to double actual damages at a court's discretion, as punitive damages.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

All rights of the data subject can be exercisable through both the judicial system and enforced by the supervisory authority.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

The Personal Data Protection Act BE 2562 (2019) does not include any derogations, exclusion or limitations other than those already described.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

There is no specific requirement or restriction that applies to cookies or equivalent technology in Thailand. However, a service provider of any website will be regarded as a PI controller according to the Personal Data Protection Act BE 2562 (2019) (PDPA). Therefore, such service providers must comply with provisions prescribed in the PDPA.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

Currently, there are no specific requirements and restrictions that apply to electronic communications marketing in Thailand. Nonetheless, we advise that providers of any such services or platforms who will be regarded as data controllers according to the PDPA must comply with provisions prescribed in the PDPA; namely, the service provider might have to request for PI owner's consent before collection, use and disclosure of PI.

FOSR

John P Formichella
john@fosrlaw.com

Naytiwut Jamallsawat
naytiwut@fosrlaw.com

Onnicha Khongthon
onnicha@fosrlaw.com

399, Interchange 21 Building, 23rd Floor
Unit 3, Sukhumvit Road
Klongtoey-Nua
Wattana
Bangkok 10110
Thailand
Tel: +662 107 1882
www.fosrlaw.com

Targeted advertising

42 | Are there any rules on targeted online advertising?

Currently, there are no specific requirements or restrictions that apply to targeted online advertisement in Thailand. However, we assume that targeted advertising requires PI from an individual specifically, and thus, a service provider of such service will be regarded as data controller according to the PDPA. Therefore, such service providers must comply with provisions prescribed in the PDPA; namely, the service provider might have to request for PI owner's consent before collection, use and disclosure of PI.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Under Thailand personal data protection laws, the sensitive personal information can be collected, used or disclosed only if a PI owner gives explicit consent to the PI controller, unless such collection, use or disclosure are for scientific, historical or statistical purposes and suitable measures have been taken to protect the fundamental rights of the owner.

In this regard, if the PI owner has concerns about whether such collection, use and disclosure is necessary or not, the PI owner has the right to object unless it is for reasons of public interest.

Profiling

44 | Are there any rules regarding individual profiling?

Currently, there are no specific requirements or restrictions that apply to profiling in Thailand. However, we assume that profiling comprises direct and indirect PI from the owner. Therefore, a service provider who will be regarded as data controller according to the PDPA must comply with provisions prescribed in the PDPA; namely, the service provider might have to request the PI owner's consent before collection, use and disclosure of PI.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Currently, there are no rules or regulator guidance on the use of cloud computing services prescribed under the PDPA. However, a cloud computing service provider may be regarded as a PI owner or PI processor according to the PDPA. Therefore, a cloud computing service provider must comply with the provisions prescribed in the PDPA accordingly.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

As the Personal Data Protection Act BE 2562 (2019) (PDPA) has been effective since 1 June 2022, business operators should prepare themselves to comply with the duties of a data controller under the PDPA. First, a business operator has to determine whether the PDPA applies to its organisation and activities. Then, if the PDPA applies, a business operator should map a data flow (ie, what data the organisation collects and how the data is being used) and provide a privacy notice to inform data subjects of the personal data collected.

Regarding future collection, disclosure, and use of personal data, business operators should identify the legal basis for the collection, use, or disclosure to determine whether consent from data subjects is required or not. A data controller will need to provide a privacy notice and request a consent form (if needed) from the data subject.

Turkey

Esin Çamlıbel, Beste Yıldızili Ergül, Naz Esen and Canberk Taze

Turunç

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Turkish Constitution has specifically protected PI since 2010.

The protection of PI has also been regulated by specific legislation, namely the Personal Data Protection Law (PDPL), Law No. 6698, which came into force in October 2016. Directive 95/46/EC is the starting point for the PDPL. Even though there are various differences between the PDPL and the EU General Data Protection Regulation (GDPR), the PDPL is generally based on, and follows, the GDPR.

Turkey is a party to the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data of 1981 of the Council of Europe. The Convention was published in the Turkish Official Gazette in March 2016 and became domestic law.

Crimes against data protection and related sanctions are also regulated by the Turkish Criminal Code.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The authority responsible for overseeing the implementation of the PDPL is the Personal Data Protection Authority (the Authority). The Authority is responsible, among other things, for monitoring the latest developments in legislation and practice, making evaluations and recommendations, conducting researches and analyses, and cooperating with public institutions and organisations, international organisations, non-governmental organisations, professional associations and universities.

The Data Protection Board (the Board) is formed within the Authority and has the following duties, among others:

- ensuring that personal data are processed in compliance with the PDPL, and fundamental rights and freedoms;
- promulgating rules and regulations under the PDPL;
- determining administrative sanctions under the PDPL;
- reviewing complaints of PDPL violations;
- taking necessary measures against PDPL violations at its discretion;
- setting a strategic plan for the Authority;
- determining the purpose, targets, service quality standards and performance criteria of the Authority;
- determining additional measures for the processing of sensitive personal data;
- determining specific rules regarding data security, and the duties, powers and responsibilities of data controllers;
- providing comments on legislation and rules drafted by other institutions and organisations that include personal data provisions; and
- approving and publishing periodic reports on the performance, financial situation, annual activities and other matters related to the Authority.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Authority is the solely authorised institution under the PDPL. The PDPL tasks the Authority with monitoring and evaluating international developments on personal data issues, and cooperating with international organisations and foreign counterparts.

Despite the limited number of decisions the Board has issued since its formation, the visible trend is that the Board takes decisions of the European Data Protection Board (EDPB) into account when investigating cases. However, there is no mechanism to prevent the Board from taking decisions diverging from those of the EDPB.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of the PDPL can lead to both administrative fines and criminal penalties. The Board is responsible for ensuring that personal data is processed in compliance with fundamental rights and freedoms, and reviewing complaints of data subjects. The Board can take temporary measures and other adequate measures, such as monetary sanctions, against violations.

In addition, criminal acts such as the unlawful acquisition or registration of personal data, and non-destruction of personal data when required may be subject to criminal penalties under the Turkish Criminal Code.

1.5 Judicial review of data protection authority orders

5 Can PI owners appeal to the courts against orders of the data protection authority?

Data subjects can appeal against orders of the Authority to criminal courts of peace within 15 days of the delivery of the decision.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data Protection Law (PDPL) applies to all natural persons whose personal data is processed. It also applies to all natural and legal persons who process such data using fully or partially automated means, provided that they are part of a data registry system (the 'filing system' under the EU General Data Protection Regulation), through non-automated means. There is no distinction foreseen between private sector institutions and state institutions. As such, the PDPL applies to all types of entities and persons.

However, the PDPL does not apply in the following cases:

- processing by natural persons within the scope of activities relating to either themselves or their family members living in the same household, on the condition that the data is safeguarded and not provided to third parties;
- anonymised processing for statistical, research, planning and similar purposes;
- processing for the purposes of art, history, literature and science, or as part of the exercise of freedom of speech, provided the processing does not prejudice national defence, national security, public order, public safety, economic security, privacy and other personal rights, or constitute a crime;
- processing within the scope of preventive, protective and intelligence activities by state institutions carrying out national defence, national security, public order, public safety or economic security functions; and
- processing by judicial authorities or execution authorities in relation to investigations, prosecutions, court cases, criminal proceedings, and execution and enforcement proceedings.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

No, the PDPL does not directly cover interception of communications, electronic marketing or monitoring and surveillance of the individuals. However, the Data Protection Board (Board) has issued a decision regarding the regulation of contacting individuals via email, SMS or phone calls to make advertisements, where it held that such communications are subject to the same principles under the PDPL as apply to other data processing. Accordingly, these types of communications can be made only based on consent or in reliance on an exemption.

Turkey has specific legislation that covers the interception of communications, electronic marketing, and monitoring and surveillance of individuals. For example, the Law on Electronic Communication regulates all electronic communication methods while the Law on Electronic Trade regulates electronic marketing and trade. The Regulation on Erasure, Destruction and Anonymisation of Personal Data and the Communiqué on Rules and Procedures for the Fulfilment of the Obligation to Inform determine the rules and procedures to be applied to interception of communications, electronic marketing, and monitoring and surveillance of individuals. The Board has also published guidance regarding electronic communications bearing personal information and deemed it necessary for data controllers to take reasonable measures to verify the contact information declared by the relevant data subjects (eg, sending a verification code or link to the person's registered phone number or email address). Per the Board's approach, keeping personal data accurate and up-to-date is both in the interest of the data controller and necessary to protect the fundamental rights and freedoms of the data subject. In addition, channels must be made available at all times for data subjects to update their personal data. The Criminal Code and Criminal Procedural Law regulate the sanctions in case of breach of the applicable legislation.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

There are specific rules that outline data protection rules for various areas. For example, Turkish Labour Law holds that employers are obliged to use the personal data of employees in good faith and accordance with applicable law, and not to disclose any personal data in which an employee has a legitimate interest and has requested to be kept private.

Another example is the Regulation on Processing and Maintaining Privacy of Personal Health Data, regulating the rules and procedures to be used while processing data involving health information.

Turkish Banking Law, the Law on Payment and Security Agreement Systems, Payment Systems and Electronic Currency Organisations and the Law on Bank Cards and Credit Cards regulate the processing and transfer of financial data in Turkey and abroad.

Turkish telecommunications legislation also has provisions regarding data processing and transfers.

PI formats

9 | What categories and types of PI are covered by the law?

The PDPL does not limit the scope of protection by categories or types. All information relating to an identified or identifiable natural person maintained and stored in any format is covered by the PDPL and secondary legislation promulgated thereunder. However, there are specific provisions in the PDPL that regulate sensitive personal data as 'special categories of personal data'.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The PDPL makes no differentiation between data subjects who are nationals or not. The PDPL applies to all natural persons whose personal data are processed.

However, there are specific rules that apply to the transfer of personal data outside of Turkey. As a general rule, personal data cannot be transferred abroad without the explicit consent of the data subject. However, personal data may be transferred abroad without the explicit consent of the data subject provided that one of the conditions specified in the PDPL is met, and that:

- adequate protection is provided in the foreign country where the data are to be transferred (the Board has the authority to determine the countries where an adequate level of protection is deemed to be provided although it has not done so yet); or
- where adequate protection is not provided, the controllers in Turkey and the relevant foreign country guarantee sufficient protection in writing, and the Board authorises such transfer (although data requiring data subject's explicit consent in Turkey will continue to require such consent and will not be automatically covered by the approved undertaking); or
- approved binding corporate rules are followed (although data requiring data subject's explicit consent in Turkey will continue

to require such consent and will not be automatically covered by such rules).

Hence, the applicability of the PDPL is not limited to Turkey.

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The PDPL covers all processing and use of personal data. Certain distinctions are made among the owners, controllers and processors concerning their duties and liabilities.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

As a general rule, personal data cannot be processed without the explicit consent of the data subject. However, if one of the following conditions is met, personal data may be processed without seeking the explicit consent of the data subject:

- the processing is clearly provided for by applicable law;
- the processing is necessary to protect the life or bodily integrity of a person who is unable to give consent due to actual impossibility or whose consent is not legally recognised, or the life or bodily integrity of another person;
- the processing is necessary for the formation or performance of a legal contract to which the data subject is a party;
- the processing is necessary to comply with a legal obligation to which the data controller is subject;
- the data has been made public by the data subject;
- the processing is necessary to establish, use or protect a legal right; and
- the processing is necessary for the purposes of legitimate interests pursued by the controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

Pursuant to the Data Protection Board's (the Board) recent decisions, data processors can request the explicit consent of the data owners only if the above circumstances are not present.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

Under the Personal Data Protection Law (PDPL), personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, clothing choices and habits, trade union membership, health, sex lives, criminal convictions and security measures, and biometric or genetic information are defined as 'sensitive personal data'. As a general rule, these categories of data cannot be processed without the consent of the data subject, except where permitted or required by applicable law.

Further, personal data relating to health and sex lives may be processed without the explicit consent of the data subject only by persons or authorised public institutions and organisations that have confidentiality obligations, and only to protect public health, the administration of preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of healthcare services.

Processing of data must comply with the purposes stated in the data processing notification. If the processor decides to process the data for any reason other than those stated in the data processing notification, a new notification stating the new purpose must be provided to the data subject.

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. These measures include, among others, training programmes, encryption requirements, two-factor authentication for remote access, and physical security measures, such as access controls.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

When processing personal data, the controller or the person authorised by the controller is obliged to inform the data subjects. The notification must include:

- the identity of the controller and its representative, if any;
- the purpose of the data processing;
- to whom and for what purposes the processed data may be transferred;
- the method and legal basis for the collection of the personal data; and
- the rights of the data subjects accorded by the Personal Data Protection Law (PDPL).

The notification must be provided at the time of the acquisition of the data and must use easy-to-understand clear and plain language. If the personal data are obtained from a third party (ie, not the data subject), the notification must be made within a reasonable time after the data are obtained, at the time of first contact if obtained for the purpose of communication, and at the time of first transfer if obtained for the purpose of transferring.

Exemptions from transparency obligations

15 When is notice not required?

A notice is not required if:

- processing of the personal data is necessary to prevent a crime or for a criminal investigation;
- the data subject has himself or herself made the personal data public;
- processing of the personal data is required for supervisory, regulatory or disciplinary activities to be carried out by public institutions and professional associations with public institution status; or
- processing of the personal data is required for the protection of the state's economic and financial interests with regard to budgetary, tax-related and financial issues.

Data accuracy

16 Does the law impose standards in relation to the quality, currency and accuracy of PI?

Personal data must be:

- processed lawfully and fairly;
- accurate and, where necessary, kept up to date;
- collected for specified, explicit and legitimate purposes;

- relevant and limited to the purposes for which they are processed; and
- retained only for the period stipulated by relevant legislation or the purpose for which they are processed.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

According to the PDPL, the amount of data processed must be proportional to the purpose of the processing, and the amount must be as small as possible. Any data processing that exceeds the scope of the purpose for which it was collected is unlawful. Data controllers must avoid processing data that is disproportionate to achieving the purpose of the processing (eg, avoid processing sensitive personal data when hiring, as the same purpose could be achieved without processing any or by only processing minimal personal data).

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

There is no restriction on the amount of personal data that may be held. However, personal data can be preserved only for the time periods foreseen in the applicable regulations or time periods necessary for the purpose of the processing.

In addition, the amount of data and the length of time the data may be held for must be proportional to the purpose of the processing, and both the amount of PI and the length of time must be as small as possible.

While determining the maximum storage period, the following must be taken into account:

- generally accepted storage periods in the sector in which the data controller operates;
- the length of time the legal relationship with the data subject that is the basis of the processing will continue for;
- the length of time that the legitimate interest of the data controller in accordance with lawfulness and fairness principles will continue for;
- the length of time during which the risks, costs and responsibilities arising from the storage of the relevant data category will legally continue for;
- whether the intended maximum storage period is suitable to keep the relevant data category accurate and up to date;
- the length of time during which the data controller is obliged to store the data pursuant to its legal obligations; and
- the period of limitation determined by the data controller for the assertion of a right relating to personal data in the relevant data category.

Those data controllers who are obliged to register with the Data Controllers' Registry, known as VERBİS, are also obliged to prepare a data inventory, as well as data preservation and destruction policies, which set forth, among other things, the periods during which personal data will be preserved.

Data controllers who are required to prepare data preservation and destruction policies must erase, destroy or anonymise, as applicable, the relevant data in regular intervals upon the triggering of such obligation. These periods cannot exceed six months. On the other hand, for data controllers who are not required to prepare data preservation and destruction policies, this time period cannot exceed three months.

Records of all erasure, destruction and anonymisation activities must be kept and stored for at least three years (subject to any other applicable legal obligations).

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes, the purposes for using the personal data must be determined and the data subject accordingly informed when obtaining the consent of the data subject. Data controllers cannot exceed or circumvent these purposes. Further, regardless of whether the processing of PI is based on the consent of the data owner or a legitimate ground not requiring consent, the processing purposes must be disclosed to the data subjects.

Data controllers are bound by the purposes stated in the relevant notification. Unless it is explicitly permitted by the PDPL, data controllers cannot use the data collected other than for the purposes clearly disclosed while collecting the data. Hence, if the collected data will be used for a new purpose requiring consent, data controllers are obliged to provide a new notification and to obtain a separate consent of the data subject. If the new purpose is based on one of the legitimate grounds under the PDPL (ie, no consent is necessary), data controllers still have to provide the data subject with a new notification that includes the new purpose.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

There is no prohibition for using automated decision systems or making automated decisions without human intervention. The general principles of the PDPL, such as informing the data subject, shall always apply.

Additionally, as per the PDPL, data subjects can always object to the results of automated decision-making.

SECURITY

Security obligations

21 | What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Data controllers are obliged to take all necessary technical and administrative measures to provide a sufficient level of security. Data controllers must also conduct necessary inspections or have them conducted in their own institutions. While there are no specific standards established for the technical and administrative measures to be used, the relevant guidelines of the Data Protection Board (the Board) set forth various possible data security measures. These measures include, among other things, establishing a data matrix, using closed-circuit systems, using firewalls and anti-virus programs, and implementing data security policies.

Notification of data breach

22 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Under the Personal Data Protection Law, in cases where the processed data is obtained by third parties through unlawful methods, the controller must notify the data subject and the Board as quickly as possible and, in

any event, within 72 hours. Where necessary, the Board may announce such breach on its official website or through other methods it deems appropriate.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Under the Personal Data Protection Law (PDPL), data controllers are obliged to implement all necessary technical and administrative precautions to maintain data security. While the legislation does not specifically include an obligation to maintain internal controls, data controllers who are obliged to register with the Data Controllers' Registry are also obliged to prepare data preservation and destruction policies, which must contain, among other things, extensive information on how the data will be processed internally. The Data Protection Board (the Board) also recommends signing confidentiality agreements with the employees in case of a data breach.

Further, if an international company adopts binding corporate rules, and these rules are approved by the Board to transfer personal data abroad without the explicit consent of the data subject, the company and other companies in its group will be required to set up an internal compliance mechanism in accordance with the law.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The PDPL does not foresee an obligation for appointing a data protection officer. However, the Board recently published the Communiqué on Procedures and Principles of Personnel Certification Mechanism (the Communiqué) and the Programme on Certification of Data Protection Personnel (Programme). The Communiqué and the Programme explain the certification process of data protection personnel in terms of competence and procedural requirements for accreditation. For example, data protection personnel must pass a written exam and meet the minimum requirements determined by the Board to obtain their certificates. Although the obligations of data protection personnel have not been set yet, the Board is laying the legal groundwork to implement a similar function to that of a data protection officer in the near future.

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The PDPL does not contain a provision regarding a general obligation to maintain internal records. However, data controllers and processors who process personal data by automated means are obliged to register with the Data Controllers' Registry and establish a personal data processing inventory, which must include the purpose and the legal reason for the processing, the data category, to whom the data will be transferred, the period of preservation, data to be transferred abroad, and the precautions taken for data security.

Those data controllers who are obliged to register with the Data Controllers' Registry are also obliged to prepare data preservation and destruction policies, which set forth, among other things, the periods during which personal data will be preserved.

In addition to the PDPL, the Law on Electronic Communications and related regulations oblige licensed operators within the electronic communications sector to maintain certain records relating to electronic communications. Licensed operators are also under an obligation to keep access records of personal data for two years.

Risk assessment

26 Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Data controllers are at all times obliged to take all necessary technical and administrative measures to provide a sufficient level of security. However, the Board particularly focuses on whether the personal data is sensitive, as well as the confidentiality level of the data and the possible damage to the data subject in the event of a security breach. While there are no specific standards established for the technical and administrative measures to be used, the relevant guidelines of the Board set forth various possible data security measures. These measures include, among other things, informing employees regarding possible security breaches, establishing a data matrix, using closed-circuit systems, using firewalls and anti-virus programs, and implementing data security policies.

Design of PI processing systems

27 Are there any obligations in relation to how PI processing systems must be designed?

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. However, there are no specific obligations as such in relation to PI processing systems outside of sensitive personal data.

REGISTRATION AND NOTIFICATION

Registration

28 Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

As a general rule, data controllers are required to register with the Data Controllers' Registry (VERBİS). The Data Protection Board (the Board) has exempted, through various decisions, the following data controllers from the registration requirement:

- data processors who are part of a data registry system (the 'filing system' under the EU General Data Protection Regulation) and process data only in non-automated ways;
- associations, foundations and unions resident in Turkey, to the extent they process data in compliance with relevant legislation and their purposes, and in any case, limited to their areas of activity;
- political parties;
- lawyers;
- mediators;
- notaries public;
- certified public accountants;
- customs brokers; and
- employers who employ fewer than 51 people and whose annual net assets do not exceed 25 million Turkish lira, provided their primary line of business is not the processing of sensitive personal data.

Data controllers who are not exempt from the obligation to register must register with VERBİS at verbis.kvkk.gov.tr. As part of the registration process, data controllers must appoint a contact person and

complete the form provided by the Personal Data Protection Authority. If the data controller is in a foreign country, a data controller representative resident in Turkey must be appointed.

The following information must be registered with VERBİS by the data controller:

- the identity and address of the data controller and of its representative (if any);
- the purpose for which the personal data will be processed;
- explanations relating to the groups of data subjects and the relevant data categories of the subjects;
- the recipients or groups of recipients to whom the personal data may be transferred;
- the personal data envisaged to be transferred abroad;
- the measures taken concerning the security of the personal data; and
- the maximum storage period necessary for the purpose for which the personal data are processed.

Registration and renewals are not subject to any fees.

Persons who fail to comply with the obligation to register with and maintain proper entries on VERBİS may be sanctioned with a monetary fine between 50,000 Turkish lira and 2.7 million Turkish lira by the Board.

Other transparency duties

29 | Are there any other public transparency duties?

Public companies have a general duty to disclose information on events that may affect their investors' decisions. While this requirement is not specifically regulated for data processing, matters relating to data privacy will need to be disclosed if sufficiently material. There are no other transparency duties; data processors are only obliged to notify the data subjects as required by the PDPL and register with VERBİS when the applicable conditions are met.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Personal Data Protection Law (PDPL) foresees special conditions for the domestic transfer of personal data. Personal data normally cannot be transferred without a legitimate ground specified in the PDPL or the explicit consent of the data subject. Hence, the data controller must notify the data subject that personal data will be transferred to third parties providing outsourced processing services, and obtain the data subject's consent if the transfer is not based on a legitimate ground (such as advertising purposes). If the data subject denies providing consent and the processing is not based on a legitimate ground, the applicable personal data must be destroyed (or, if applicable consent or grounds exist, used by the data processor without the involvement of the outsourced service). Further, for personal data required to be preserved pursuant to various legislation, data owners are required to establish a system for preserving such personal data without transferring it to third parties.

The PDPL also requires that data owners who use outsourced processing services provide sufficient protection with regard to the processing and preservation of personal data. In the event of a breach, data owners are jointly and severally liable with the entities providing outsourced processing services for the compensation of any damages.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

As a general rule, there are no specific restrictions foreseen on the sharing of personal data apart from the general requirements on notifying and informing the data subject, obtaining the data subject's consent (except the conditions specified in the PDPL pursuant to which personal data can be transferred within Turkey without obtaining explicit consent) as to what data will be disclosed, and determining the purposes for which the data shall be disclosed.

However, for sharing sensitive personal data, the Data Protection Board (the Board) has set forth additional precautions and restrictions. These include the transfer of data in an encrypted format and for hard copies of the data to be labelled as classified. In addition, it is mandatory to obtain the data owner's consent unless the processing is required by law. In its guidelines, the Board specifically refers to the selling of sensitive personal data as a data breach, and Turkish Criminal Law states that the person who gives, distributes or seizes personal data unlawfully is punished with imprisonment from two to four years.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

As a general rule, personal data cannot be transferred abroad without the explicit consent of the data subject. However, personal data may be transferred abroad without the explicit consent of the data subject provided that one of the conditions specified in the PDPL is met, and that:

- adequate protection is provided in the foreign country where the data is to be transferred (the Board has the authority to determine the countries where an adequate level of protection is deemed to be provided although it has not done so yet);
- where adequate protection is not provided, the controllers in Turkey and in the relevant foreign country guarantee sufficient protection in writing, and the Board authorises such transfer (although data requiring the data subject's explicit consent in Turkey will continue to require such consent and will not be automatically covered by the approved undertaking); or
- approved binding corporate rules are followed (although data requiring data subject's explicit consent in Turkey will continue to require such consent and will not be automatically covered by such rules).

Binding corporate rules became available as an option only recently, pursuant to a Board decision. To use this method, group companies operating outside of Turkey in countries that are not listed as safe jurisdictions, must apply to the Board and submit an undertaking on their use of sufficient protection. If this undertaking is approved by the Board, then the relevant company is no longer obliged to obtain approval for each transfer.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes, if transfers outside of Turkey are subject to restriction or authorisation, these will also apply to transfers to service providers and onwards transfers.

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

The PDPL does not require the PI or a copy of PI to be retained in Turkey. However, certain regulatory bodies, such as the Capital Markets Board of Turkey and Central Bank of Republic of Turkey, often require companies subject to their enforcement to have their own information systems and, therefore, keep PI in Turkey.

RIGHTS OF INDIVIDUALS

Access

35 Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Personal Data Protection Law (PDPL), everyone has the right to:

- learn whether or not his or her personal data has been or are being processed;
- request information as to the processing if his or her data has been processed;
- learn the purpose of the processing and whether data is used in accordance with such purpose; and
- know the identity of the third parties in Turkey and abroad to whom personal data has been transferred.

Data subjects can use these by directly applying to the data controller in writing (in Turkish). Data controllers are obliged to respond to requests within 30 days. There are no limitations or fees associated with exercising these rights, except that the data controller may pass on any costs it incurs (eg, cost of a flash drive sent to the data subject).

Other rights

36 Do individuals have other substantive rights?

Each data subject has the right to apply to the controller and:

1 request the rectification of any incomplete or inaccurate data;
2 request the erasure or destruction of his or her personal data (subject to the conditions specified in the PDPL);
3 request notification of the actions listed in (1) and (2) to third parties to whom his or her personal data has been transferred;
4 object to any unfavourable result or consequence for the data subject, if such result or consequence is the result of exclusively automated means of the processing of his or her personal data; and
5 request compensation and other remedies for damages arising from any unlawful processing of his or her personal data.

Compensation

37 Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes. Despite of the fact that the PDPL does not foresee any compensation for data subjects who are affected by breaches of the PDPL, individuals can resort to general provisions of law and claim material and moral damages foreseen by the Turkish Code of Obligations. To claim material damages, the data subject must prove that a damage has occurred due to the fault of the data controller. On the other hand, to claim moral damages, the data subject must demonstrate that there was a violation of his or her individual rights and freedoms, and that violation has caused grave psychological harm.

Enforcement

38 Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Data subjects may demand that their rights in the PDPL, such as the right to be informed whether their PI is being processed, the purpose of the processing and whether the PI is being transferred to third parties to be enabled and enforced by the data controller. If the data controller does not comply with a data subject's request within 30 days, the data subject can request the relevant rights to be enforced by the Personal Data Protection Authority. Compensation claims are subject to the jurisdiction of civil courts and criminal complaints to the jurisdiction of criminal courts.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 Does the law include any derogations, exclusions or limitations other than those already described?

The Personal Data Protection Law does not include any derogations, exclusions or limitations other than those already described.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 Are there any rules on the use of 'cookies' or equivalent technology?

Electronic communications, in general, are regulated by the Information and Communication Technologies Authority (ICTA), established in accordance with Law on Electronic Communications. Per the Law on Electronic Communications, the ICTA regulates and supervises the processing and protection of personal data acquired via electronic means.

Despite the fact that there is no explicit legislation on the use of cookies or equivalent technology in the Law on Electronic Communications or other legislation, because applicable legislation does not distinguish between the means of obtaining data, any personal data obtained through cookies or similar technology is under the protection of the law, and data controllers must comply with the rules applicable to the processing of personal data when using cookies or similar technology.

However, in January 2022, the Data Protection Board (the Board) published the Draft Guide Regarding Cookie Applications (the Draft Guide) and received feedback on it. The Draft Guide provides data controllers and data subjects with clarification on which types of cookies require explicit consent and how data subjects should be informed when they enter a website. Most importantly, the Draft Guide suggests that data controllers are not required to obtain explicit the consent of the data subjects for first-party analytical cookies.

Electronic communications marketing

41 Are there any rules on marketing by email, fax telephone or other electronic channels?

The Law on the Regulation of Electronic Trade regulates the rules and conditions for marketing via electronic means.

For a data controller to use personal data for marketing by any means, the explicit consent of the data subject must be obtained. Data

subjects can always, without providing any reason, request the termination of electronic marketing communications from the data controller. Data controllers are obliged to terminate within three days all electronic communications with data subjects who require termination. Data controllers are also required to take all necessary means to preserve and protect the acquired personal data, and cannot distribute or disclose personal data without the explicit consent of the data subjects.

Further, the provision of services or sale of goods cannot be made subject to the consent to the collection of personal data that is not necessary for the provision of the relevant service or the making of the relevant sale.

The Board has also published guidance regarding electronic communications bearing personal information and deemed it necessary for data controllers to take reasonable measures to verify the contact information declared by the relevant data subjects (eg, sending a verification code or link to the person's registered phone number or email address).

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules or regulations regarding targeted online advertising. However, general principles shall always apply. As targeted online advertising does not fall under the scope of legitimate processing under the law, personal data can only be processed with the data subject's explicit consent. Likewise, this is the case for online behavioural advertising as most of the personal data is collected through cookies for targeted online advertising.

Although there are no regulations or other guidance published by the Board regarding the use of targeting and advertisement cookies, general rules require data controllers to obtain explicit consent from data subjects while the data subjects are using the data controller's website. Thus, targeted online advertising can only be done with the data subject's explicit consent.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

As a general rule, sensitive personal information cannot be processed without the consent of the data subject, except where permitted or required by applicable law. Further, personal data relating to health and sex lives may be processed without the explicit consent of the data subject only by persons or authorised public institutions and organisations that have confidentiality obligations, and only for the purposes of protecting public health, the administration of preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of healthcare services.

Processing of data must be in compliance with the purposes stated in the data processing notification. If the processor decides to process the data for any reason other than those stated in the data processing notification, a new notification stating the new purpose must be provided to the data subject.

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. These measures include, among others, training programmes, encryption requirements, two-factor authentication for remote access and physical security measures such as access controls.

TURUNÇ

Esin Çamlıbel
ecamlibel@turunc.av.tr

Beste Yıldızili Ergül
byildizili@turunc.av.tr

Naz Esen
nesen@turunc.av.tr

Canberk Taze
ctaze@turunc.av.tr

Teşvikiye Caddesi 19/11
Teşvikiye 34365
Istanbul
Turkey
Tel: +90 212 259 45 36
Fax: +90 212 259 45 38

Cumhuriyet Bulvarı 140/1
Alsancak 35210
Izmir
Turkey
Tel: +90 232 463 49 07
Fax: +90 232 463 49 09

www.turunc.av.tr

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific rules or regulations for individual profiling. However, general principles shall always apply for individual profiling. Thus, if the processing (profiling) is done for commercial purposes, in addition to the duty to inform the data subject regarding the purpose of processing, which data is being processed and whether the data controller is processing personal data through automated means, explicit consent of the data subject must be obtained.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Various pieces of legislation apply to the use of cloud computing services, including:

- the Universal Services Law;
- the Electronic Communications Law;
- the Regulation on Electronic Communications Infrastructure and Information Systems; and
- the Regulation on Rules on the Operations, Work and Supervision of Data Storage Institutions.

Furthermore, the ICTA regulates the use of cloud computing services.

However, the Turkish government's policy preference is the storage of personal data in Turkey.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In early 2021, the Data Protection Board (the Board) approved, for the first time, a number of applications for the transfer of data abroad through the use of written undertakings. Under this method, the controllers in Turkey and the relevant foreign country guarantee sufficient protection in writing, and the Board must approve such undertakings. This is a welcome development because the Board has yet to publish a list of safe jurisdictions (ie, foreign countries deemed to provide an adequate level of protection), another permitted (but not currently usable) method of transferring data abroad.

Binding corporate rules also became available as an option to transfer data abroad. To use this method, group companies operating outside of Turkey in countries that are not listed as safe jurisdictions must apply to the Board and submit an undertaking on their use of sufficient protection. If this undertaking is approved by the Board, then the relevant company is no longer obliged to obtain approval for each transfer.

In December 2021, the Board published the Communiqué on Procedures and Principles of Personnel Certification Mechanism and the Programme on Certification of Data Protection Personnel. Although the obligations of data protection personnel have not been set yet, we understand that the Board is laying the legal groundwork to implement a similar function to that of a data protection officer in the near future.

In January 2022, the Board published the Draft Guide Regarding Cookie Applications (the Draft Guide) and received feedback on it. The Draft Guide informs data controllers and data subjects on which type of cookies require explicit consent and how the data subject must be informed when they enter a website. Most importantly, the Draft Guide suggests that data controllers are not required to obtain explicit consent of the data subjects for first-party analytical cookies.

United Arab Emirates

Saifullah Khan and Saeed Hasan Khan
BIZILANCE LEGAL CONSULTANTS

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 | Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The following laws and regulations make up the legal framework to govern data privacy in the United Arab Emirates (UAE):

- Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law): this law is applicable across the UAE, except for in free zones, which have their own legislation on personal data protection;
- Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law): this law is applicable in the DIFC (the DIFC is a free zone); and
- the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations): these regulations are applicable in the ADGM (the ADGM is also a free zone).

The above laws largely follow the EU General Data Protection Regulation.

Data protection authority

2 | Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The UAE Law

The UAE Data Office (the Data Office) is responsible for enforcing data privacy under the UAE Law. The Data Office is competent to receive and decide the complaints of data subjects regarding contravention of the provisions of the UAE Law. The Data Office is also competent to impose administrative sanctions.

The DIFC Law

The Commissioner of Data Protection for the DIFC (the DIFC Commissioner) administers the DIFC law. The DIFC Commissioner is empowered to receive and decide complaints concerning the contravention of the DIFC law. The DIFC Commissioner is also empowered to investigate complaints and to issue directions or declarations on the complaints and impose fines.

The ADGM Regulations

The Commissioner of Data Protection for the ADGM (the ADGM Commissioner) is responsible for enforcement of the ADGM Regulations. The ADGM Commissioner is empowered to receive and decide complaints regarding the contravention of the ADGM Regulations and to impose fines.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Data Office is competent to propose joining or signing international conventions and agreements and to propose partnership agreements with the Gulf, regional and international states, organisations and bodies with respect to the activities and competencies of the Data Office. This is done in coordination with the Ministry of Foreign Affairs and International Cooperation.

The DIFC Commissioner and the ADGM Commissioner are empowered to participate in and cooperate with other data protection authorities.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches are brought before the concerned authority (the Data Office, the DIFC Commissioner or the ADGM Commissioner, as the case may be), which is empowered to levy fines. Orders and directions of the respective authority are appealable before the concerned courts.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

The UAE Law

A complaint must first be filed with the Data Office. Grievances against any decision, administrative sanction or action of the Data Office must be filed with the Director General of the Data Office. A decision, administrative sanction or action of the Data Office may not be appealed unless a grievance is filed with the Director General of the Data Office.

The DIFC Law and the ADGM Regulations

A complaint must first be submitted to the DIFC Commissioner or the ADGM Commissioner. The disputes are heard in appeal before the DIFC courts or the ADGM courts, respectively.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The UAE Law

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) is not applicable to the following:

- government data;
- government authorities that control and process personal data;
- security and judicial authorities;
- data subjects processing data related to them for personal purposes;
- personal health data;
- personal banking and credit data; and
- companies and organisations incorporated in free zones.

Except the above, the UAE Data Office (the Data Office) has the power to exempt certain establishments that do not process a large volume of personal data from any or all requirements of the UAE Law, in accordance with the standards and controls to be specified by executive regulations.

The DIFC Law

The Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) is not applicable to the processing of personal data by natural persons in the course of purely personal or household activity that has no connection to a commercial purpose. The DIFC Board of Directors may make regulations to exempt controllers from compliance with the DIFC Law (or any part thereof). Certain provisions of the DIFC Law are not applicable to DIFC bodies. DIFC bodies are the DIFC Authority, the Dubai Financial Services Authority, the DIFC courts and any other person, body, office, registry or tribunal established under DIFC law or established upon approval of the President of the DIFC that is not revoked by the DIFC Law of by any other DIFC law.

The ADGM Regulations

The Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations) are not applicable to the processing of personal data by a natural person for the purposes of purely personal or household activity. In addition, the ADGM Regulations are not applicable to the processing of personal data by public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to national security.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The data protection laws do not cover the interception of communications or surveillance. However, they provide a right to the data subjects to not to be subjected to automated decision-making, including profiling in the context of electronic marketing.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

Sector-specific framework concerning protection of personal data is as follows:

- banking: Federal Law No. 14 of 2018 (concerning the Central Bank of the UAE) governs data protection for bank customers;
- telecommunications: Federal Law No. 3 of 2003 (concerning telecommunications) governs data protection for telecom consumers; and
- health: Federal Law No. 2 of 2019 (concerning use of information and communication technology in health fields) governs the confidentiality of patient information.

PI formats

9 | What categories and types of PI are covered by the law?

The data protection laws are applicable to the processing of personal data irrespective of processing by automated means or otherwise.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The laws have an extraterritorial effect as follows:

- The UAE Law is applicable to:
  - a data controller or processor established in the UAE that carries out personal data processing for data subjects who are outside the UAE; and
  - a controller or processor not established in the UAE that carries out the personal data processing of data subjects who are in the UAE.
- The DIFC Law is applicable to a controller or processor, regardless of its place of incorporation, that processes personal data in the DIFC.
- The ADGM Regulations are applicable in the context of activities for the establishment of a controller or processor in the ADGM, regardless of whether the processing takes place in the ADGM.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Processing by the controller or the processor is covered under data protection laws. The data protection laws provide the responsibilities of the controllers and the processors.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The UAE Law

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) prohibits the processing of personal data without the consent of the data subject (certain exceptions apply). Processing must:

- be fair, transparent and lawful;
- be carried out for the purpose specified;
- be adequate and relevant;
- be correct, accurate and up to date;
- ensure erasure or rectification of incorrect data;
- be safe and secure;

- not store the personal data after the completion of the purpose for which it was collected (it may be maintained if the identity of the data subject is anonymised); and
- be in accordance with any other controls as may be specified by executive regulations.

The DIFC Law and the ADGM Regulations

Data may be collected lawfully:

- with the consent of the data subject;
- when necessary for the performance of a contract to which the data subject is a party;
- when necessary for compliance with the applicable law to which the controller is subject;
- when necessary to protect the vital interests of a data subject or another natural person;
- when necessary:
  - for the performance of a task carried out by a DIFC body or public authority in the interest of the ADGM;
  - in the exercise of powers and functions of a DIFC body, the ADGM, the Financial Services Regulatory Authority, the ADGM courts and the Registration Authority; or
  - in exercise of powers and functions vested by a DIFC body by a third party to whom personal data is disclosed by the DIFC body; and
- when necessary for the purposes of legitimate interests pursued by a controller or a third party, except where these interests are overridden by the interests or rights of a data subject.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

'Sensitive personal data', under the UAE Law, means any information that directly or indirectly reveals a person's race, ethnicity, political or philosophical views, religious beliefs, criminal record, biometric data, or any data related to a person's physical, psychological, mental, corporal, genetic or sexual health, including information related to a person's healthcare that reveals their health conditions.

'Special categories of personal data', under the DIFC Law, means personal data revealing or connecting (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal records, trade union membership and health or sex life, including genetic and biometric data where it is used for the purpose of uniquely identifying a natural person.

The ADGM Law has a similar definition of special categories of personal data as the DIFC Law.

The UAE Law states that a personal data protection impact assessment is necessary where processing involves a large volume of sensitive personal data.

The DIFC Law and the ADGM Regulations permit the processing of special categories of personal data in certain specified situations, including:

- with the explicit consent of the data subject;
- where processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the controller or data subject concerning employment;
- where processing is necessary to protect the vital interests of the data subject;
- where processing is carried out by a foundation, association or any other non-profit in the course of its legitimate activities;
- where processing is related to personal data that has been made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for compliance with a specific requirement of a law applicable to the controller.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) does not have any such requirement.

The DIFC Law and the ADGM Regulations

In the Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) and the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations) there is a requirement to provide information to the data subject when personal data is obtained from them and when personal data has not been obtained from them. The information required to be provided to the data subject includes:

- the identity and contact details of the controller;
- the contact details of the data protection officer (where applicable);
- the purpose and lawful basis of processing;
- the legitimate interest of the controller (where applicable);
- the types of personal data that are being processed;
- the categories of the recipients of the personal data;
- safeguards in the case of the transfer of personal data to any other jurisdiction or to an international organisation;
- the period for which the personal data will be stored;
- the rights of the data subject; and
- the source the personal data is obtained from (when personal data is not obtained from the data subject).

The information is to be provided in writing, including, where applicable, by electronic means.

Exemptions from transparency obligations

15 | When is notice not required?

Information the data subject already has need not be provided when personal data is obtained by the data subject.

When personal data is not obtained by the data subject, the information providing provision is not applicable in following cases:

- the data subject already has the information;
- the provision of information proves impossible or would involve a disproportionate effort;
- where disclosure is expressly required by applicable law; and
- where personal data must remain confidential subject to the obligation of professional secrecy or the duty of confidentiality in accordance with applicable law.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

The data protection laws require that personal data is kept accurate and up to date.

Data minimisation

17 Does the law restrict the types or volume of PI that may be collected?

The data protection laws require that personal data is relevant and limited to what is necessary for the purpose for which it is being processed.

Data retention

18 Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The UAE Law

The UAE Law requires that personal data not be stored after the completion of the purpose of its processing. The UAE Law further provides that personal data may be maintained (after the completion of the purpose for which it was gathered) if the identity of the data subject is concealed through anonymisation.

The DIFC Law and the ADGM Regulations

The controller and the processor are required to have policies and processes to securely and permanently delete, anonymise, pseudonymise and encrypt personal data or prevent it from being used further when grounds for data retention no longer apply.

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The data protection laws provide that personal data must be processed for a clear, specified, explicit and legitimate purpose. The processing must not be incompatible with the stated purposes.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The data subject has the right to object to automated decision-making (including profiling) that has legal implications or consequences affecting a data subject.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

According to Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law), the controller and processor must put in place and implement appropriate technical and organisational measures and actions to ensure a high level of security that is appropriate to the risks associated with the processing. These measures must be in accordance with the best international standards and practices.

According to Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) and the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations), the controllers (and processors, where applicable) are required to implement appropriate technical and organisational measures to protect the personal data. In addition, controllers are required to ensure the security of personal data by following the principles of data protection by design and data protection by default.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The data controller is required to notify a data breach to the UAE Data Office (the Data Office), the Commissioner of Data Protection for the DIFC (the DIFC Commissioner) and the Commissioner of Data Protection for the ADGM (the ADGM Commissioner) when the breach is likely to result in a risk to the privacy, confidentiality, security or rights of the data subjects. The processor must notify, without delay, any such breach to the controller.

The UAE Law requires immediate notification of the breach. The DIFC Law requires notification of the breach as soon as practicable in the circumstances. The ADGM Regulations require that breach notification be made within 72 hours of having become aware of the breach, and, if notification is not made within 72 hours, then reasons of delay must also accompany the breach notification.

The breach notification must contain at least the following information:

- a description of the nature of the breach;
- the details of the data protection officer;
- the likely effects and consequences of the breach;
- a description of the measures taken or proposed to be taken by the controller to rectify or remedy the breach and the measures to mitigate its effects; and
- any other requirement of the Data Office (only in case of the UAE Law).

Where a breach is likely to result in a high risk to the security or rights of a data subject, the controller is also required to notify the breach to the data subject.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

According to Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law), the controller and processor must put in place and implement appropriate technical and organisational measures and actions to ensure a high level of security that is appropriate to the risks associated with the processing. These measures must be in accordance with the best international standards and practices.

According to Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) and the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations), the controllers (and processors, where applicable) are required to implement appropriate technical and organisational measures to protect the personal data. In addition, controllers are required to ensure the security of personal data by following the principles of data protection by design and data protection by default.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The requirements for the appointment of a data protection officer (DPO) are as follows.

The UAE Law

A DPO must be appointed when processing is likely to result in a high risk to the privacy and confidentiality of personal data, owing to the adoption of new technologies or the amount of data. In addition, a DPO must be appointed where the processing involves a systematic and overall assessment of sensitive personal data, including profiling and automated processing

The executive regulations will specify the kinds of technologies and standards of determination of the amount of data related to the above.

The DIFC Law

A DPO must be appointed by the Commissioner of Data Protection for the DIFC (the DIFC Commissioner), the DIFC Authority and the Dubai Financial Services Authority. Further, a DPO must be appointed by a controller or processor performing high-risk activities on a systematic or regular basis. A controller or processor may be required to designate a DPO by the DIFC Commissioner.

The ADGM Regulations

A DPO is required to be appointed where:

- the processing is carried out by a public authority (excluding courts acting in their judicial capacity);
- the core activities of a controller or processor require (on the basis of the nature, scope and purposes of processing) regular and systematic monitoring of data subjects on a large scale; and
- the core activities of a controller or processor consist of the processing of a large number of special categories of personal data.

Responsibilities of DPO

The responsibilities of a DPO include:

- monitoring the compliance of the controller or processor within the applicable legal framework;
- informing and advising the controller and processor and their respective employees (who carry out personal data processing) of their obligations under the applicable legal framework; and
- acting as a contact point for the concerned regulator.

There are no specified qualifications for the appointment of a DPO. The general requirement is having adequate skills and knowledge of the applicable data protection law.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The UAE Law

The controller must maintain the following records:

- details of the controller and the data protection officer;
- a description of categories of personal data;
- data related to persons authorised to access personal data;
- the time frame, restrictions and scope of processing;
- the erasure, modification and processing mechanisms;
- the purpose of the processing;
- data related to cross-border transfer and its processing; and
- a description of technical and organisational actions related to information security and processing.

The DIFC Law and the ADGM Regulations

The following written records must be kept:

- the name and contact details of the controller, joint controller (where applicable) and data protection officer;
- the purpose of the processing;
- a description of categories of data subjects and personal data;
- categories of recipients to whom personal data has been or will be disclosed;
- details of locations (third country) or international organisations to which personal data is transferred, including documents in relation to suitable safeguards;
- time limits for the erasure of the different categories of personal data (where possible); and
- a general description of the technical and organisational measures for the security of personal data (where possible).

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Controllers are required to undertake a data protection impact assessment before carrying out processing that is likely to result in a high risk to the rights of natural persons. In addition, the UAE Law places a mandatory requirement for a data protection impact assessment in the following cases:

- where processing involves systematic and extensive evaluation of personal aspects of the data subject that is based on automated processing (including profiling) and has legal effects that will significantly impact the data subject; and
- where processing involves a large volume of sensitive personal data.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The UAE Law

The UAE Law does not specifically mention the concept of privacy by design or privacy by default. However, it requires that a controller implement appropriate technical and organisational measures and actions for the protection and security of personal data to ensure that personal data is not subject to breach, corruption, modification or manipulation.

The DIFC Law

The requirement under the DIFC Law is that processing must be designed to reinforce data protection principles at the time of determining the means for processing and the time of processing, that personal data that is necessary for each specific purpose must be processed and that personal data must not made accessible to an indefinite number of persons without intervention of the data subject.

The ADGM Regulations

The ADGM Regulations require that a controller must take appropriate steps to ensure that their systems, business processes and practices are designed taking into account compliance with principles, rights and obligations of the ADGM Regulations. The controller must further ensure that only personal data that is necessary for each specific purpose is processed.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no requirement for the registration of controllers or processors under Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law).

Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) requires that a controller or processor register with the Commissioner of Data Protection for the DIFC (the DIFC Commissioner). The DIFC Law requires that a controller or a processor notify the DIFC Commissioner of the following processing operations:

- the processing of personal data;
- the processing of special category data; and
- the transfer of personal data to a recipient outside the DIFC that is not subject to the laws and regulations that ensure an adequate level of protection.

The registration process is online and must be renewed annually. The maximum fine under the DIFC Law for failure to register or notify is US$25,000.

The ADGM Regulations require that a controller pay a data protection fee and provide (to the Commissioner of Data Protection for the ADGM) its name and address and the date it commenced processing personal data. The ADGM Regulations do not provide for a specific sanction or fine for failure to register or notify. The registration process is online and must be renewed annually. The maximum general administrative fine is up to US$28 million for committing a prohibited act or omitting to carry out an act.

Other transparency duties

29 | Are there any other public transparency duties?

No further duties are applicable.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The UAE Law

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) requires that controllers appoint processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that provisions of the UAE Law could be met. The processor must process the personal data on instruction from the controller and pursuant to the contract between the controller and the processor. This contract must identify the scope, subject, purpose, nature and type of personal data and the categories of the data subject.

The DIFC Law and the ADGM Regulations

According to Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) and the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations), processing by a processor is governed by a legally binding written agreement between the controller and the processor. A processor must provide sufficient assurances and guarantees that it will implement appropriate technical and organisational measures to ensure that processing meets the legal requirements and to ensure the protection of rights of the data subjects.

According to the DIFC Law, the agreement between the controller and the processor must contain, among other things:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subjects;
- the obligations and rights of the controller;
- commitment by the processor to process personal data based on documented instructions from the controller; and
- assurance that persons authorised to process relevant personal data are under legally binding written agreements or duties of confidentiality.

According to the ADGM Regulations, the agreement between the controller and the processor must contain, among other things:

- that the processor is to process the personal data only on documented instructions from the controller;
- assurance that persons authorised to process personal data have committed themselves to confidentiality;
- taking into account the nature of the processing, assistance to the controller through appropriate technical and organisational measures; and
- at the choice of the controller, that all personal data will be deleted or returned to the controller after the provision of services.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The UAE Law does not have any specific provisions related to the sharing of personal data.

The DIFC Law and the ADGM Regulations

When a controller or processor receives a request from a public authority for the disclosure of personal data, the controller or processor should:

- exercise reasonable caution and diligence to determine the validity and proportionately of the request;
- assess the impact of the data transfer; and
- obtain appropriate assurance from the public authority (where reasonably practicable) that it will respect the rights of the data subjects.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The UAE Law

The UAE Law provides that personal data may only be transferred outside the UAE to a jurisdiction that has a law in place covering various aspects of the protection of personal data (providing an adequate level of protection). The personal data may also be transferred to those countries with whom the UAE has bilateral or multilateral agreements regarding personal data protection.

In the absence of adequate protection under the UAE Law, personal data may be transferred outside the UAE in the following cases (subject to controls to be specified by the executive regulations):

- in jurisdictions where data protection law does not exist, if there is a contract or an agreement binding the establishment (to whom the personal data is being transferred) to follow the provisions, measures, controls and conditions of the UAE Law – this contract or agreement must also specify a supervisory or judicial entity in that foreign country that may impose appropriate measures against the controller or processor in that foreign country if necessary;

- with the express consent of the data subject, in such a manner that does not conflict with the public and security interest of the UAE;
- when transfer is necessary for performing obligations and establishing rights before judicial entities;
- when transfer is necessary for entering into or performing a contract between the controller and the data subject, or between the controller and a third party for the interests of the data subject;
- when transfer is necessary for the performance of an act relating to international judicial cooperation; and
- when transfer is necessary for the protection of public interest.

The DIFC Law

The DIFC Law provides that personal data may be transferred abroad if there is an adequate level of protection in the foreign country, as determined by the Commissioner of Data Protection for the DIFC. There is a list of adequate jurisdictions in the DIFC Data Protection Regulations.

The ADGM Regulations

The ADGM Regulations allow the transfer of personal data abroad where the Personal Data Commissioner has decided that the receiving jurisdiction ensures an adequate level of protection. A list of jurisdictions designated as having an adequate level of protection is available on the website of the ADGM Office of Data Protection.

Transfer on the basis of appropriate safeguards – the DIFC Law and the ADGM Regulations

In the absence of an adequate level of protection, personal data may be transferred abroad if there are appropriate safeguards in place. Appropriate safeguards include:

- a legally binding instrument between public authorities;
- binding corporate rules;
- standard data protection clauses;
- an approved code of conduct; and
- an approved certification mechanism.

Specific derogations – the DIFC Law and the ADGM Regulations

In the absence of an adequate level of protection and appropriate safeguards, the data may be transferred outside of the UAE when the transfer:

- has the explicit consent of the data subject;
- is necessary for the performance of a contract between a data subject and a controller;
- is necessary for the conclusion or performance of a contract between a controller and a third party, which is in the interest of data subject;
- is necessary for reasons of public interest;
- is necessary in accordance with an applicable law;
- is necessary for the establishment, exercise or defence of a legal claim;
- is necessary to protect the vital interests of a data subject or of other persons where a data subject is physically or legally incapable of giving consent;
- is made in compliance with the applicable law and data minimisation principles to provide information to the public and is open for viewing by the public in general or by a person who can demonstrate a legitimate interest (under the DIFC Law only);
- is necessary for compliance with any obligation under the applicable law to which the controller is subject or the transfer is made at the reasonable request of a regulator, the police or another government agency or the competent authority (under the DIFC Law only);
- is necessary to uphold the legitimate interests of a controller (in international financial markets), subject to international financial standards, except where these interests are overridden by the legitimate interest of the data subject (under the DIFC Law only); and
- is necessary to comply with applicable anti-money laundering or counterterrorist financing obligations applicable to a controller or a processor (under the DIFC Law only).

Further transfer

33 If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Transfers outside the UAE to service providers are subject to the same restrictions as those not made to service providers.

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no requirement for data localisation, except for with health information and data, which – under Federal Law No. 2 of 2019 – may not be stored, processed, generated or transferred outside the UAE, except on a decision issued by the Health Authority in coordination with the Ministry of Health and Prevention.

RIGHTS OF INDIVIDUALS

Access

35 Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Data subjects have the right to access their personal data.

The UAE Law

The controller must provide clear and appropriate means and mechanisms enabling the data subjects to communicate and request to exercise their rights provided under Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law).

The data controller has a right to reject the request in following cases:

- the request is not related to information that is subject to access under the UAE Law or is excessively repeated;
- the request is in contravention of judicial procedures or investigations carried out by the competent entities;
- the request has a negative impact on a controller's endeavours to protect information security; and
- the request relates to the privacy and confidentiality of personal data of a third party.

The DIFC Law

According to Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law), the controller is required to make available at least two methods to access personal data (including, but not limited to, post, telephone, email or an online form), which must not be onerous to do. Where a controller maintains a website, at least one form of contact must be available free of cost through the website and without any requirement to create an account of any sort.

A controller may restrict, wholly or partly, the provision of information to the data subject if the restriction is a necessary and proportionate measure to:

- avoid obstructing an official or legal inquiry, investigation or procedure;

- avoid prejudicing the prevention, detection, investigation or prosecution or criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights of others.

The ADGM Regulations

There is no specific mention about the means and methods for data subjects to exercise their rights.

Restrictions to the rights of data subjects under the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations) (among others) include:

- when such rights are likely to influence national security, national defence, the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment or collection of tax or duties, or an imposition of a similar nature;
- when the right relates to information required to be disclosed by applicable law (including by court order) or in connection with legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights; and
- when providing the rights would be likely under the discharge of public functions.

Other rights

36 | Do individuals have other substantive rights?

The data subjects have the following further rights:

- the right to rectification and erasure;
- the right to withdraw consent;
- the right to restrict processing;
- the right to object to processing;
- the right not to be subjected to automated decision-making, including profiling; and
- the right of data portability.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The UAE Law does not provide for any concept of compensation in relation to a grievance of a data subject.

The DIFC Law and the ADGM Regulations provide that a data subject, who suffers material or non-material damage as a result of contravention of the applicable law and regulations, is entitled to compensation. The claim for seeking compensation is to be brought before the court. Compensation must not limit or affect any fine to be imposed on a controller or a processor for contravention of any provision of the applicable law and regulations.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The UAE Law

A complaint must first be filed with the UAE Data Office (the Data Office). Grievances against any decision, administrative sanction or action taken by the Data Office must be filed with the Director General of the Data Office. A decision, administrative sanction or action of the Data Office may not be challenged in appeal unless a grievance is filed with the Director General of the Data Office.

The DIFC Law and the ADGM Regulations

A complaint must first be submitted before the Commissioner of Data Protection for the DIFC or the Commissioner of Data Protection for the ADGM. Disputes are heard in appeal before the DIFC courts and ADGM courts, respectively.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

No other derogations, exclusions or exemptions apply.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Federal Decree Law No. 45 of 2021 on Personal Data Protection (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 this direct marketing.

Data Protection Law 2020 of the Dubai International Financial Centre (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 must 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 this direct marketing.

The Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations) carry the same provisions as 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.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Telecommunications and Digital Government Regulatory Authority (TDRA) has released the Regulatory Policy for Spam Electronic Communications (the Policy). The Policy requires that licensees (of the TDRA) put all practical measures in place to minimise the transmission of spam with a UAE link across their telecommunication networks. The Policy further states that licensees must not sell, supply, use, or knowingly allow access or the right to use any tools, software, hardware or mechanisms that facilitate address harvesting and the generation of electronic addresses.

Targeted advertising

42 | Are there any rules on targeted online advertising?

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 this 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 must 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 this direct marketing.

The ADGM Regulations carry the same provisions as 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.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The UAE Law states that a personal data protection impact assessment is a necessity where processing involves a large volume of sensitive personal data.

The DIFC Law and the ADGM Regulations permit processing of special categories of personal data in certain specified situations, including:

- with the explicit consent of the data subject;
- where processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the controller or the data subject concerning employment;
- where processing is necessary to protect the vital interests of the data subject;
- where processing is completed by a foundation, association or any other non-profit in the course of its legitimate activities;
- where processing is related to personal data that has been made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for compliance with a specific requirement of a law applicable to the controller.

Profiling

44 | Are there any rules regarding individual profiling?

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 this 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 must 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 this direct marketing.

The ADGM Regulations carry the same provisions as 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.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The Central Bank of the UAE, the Securities and Commodities Authority, the Dubai Financial Services Authority of the DIFC and the Financial Services Regulatory Authority of the ADGM have issued the Guidelines for Financial Institutions adopting Enabling Technologies (the Guidelines).

The Guidelines provide guidance to financial institutions on the application of the key principles covering the use of cloud computing. The Guidelines require that all application programming interfaces (APIs) be designed based on the privacy-by-design concept, to only expose relevant data elements to any party to fulfil the API purpose. The Guidelines further require that financial institutions ensure that personal data being transmitted or stored is encrypted to enable privacy and integrity.

Bizilance Consultants

Saifullah Khan
saifullah.khan@bizilancelegal.ae

Saeed Hasan Khan
saeed.hasan@bizilancelegal.ae

D 4-5, Suite 408
Al Sarab Tower, Level 15th
ADGM Abu Dhabi
United Arab Emirates
Tel: +971 52 914 1118
www.bizilance.ae

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) only came into effect on 2 January 2022, and its executive regulations are still to be announced. Controllers and processors must adjust their respective positions (with reference to the provisions contained in the UAE Law) within a period of six months following the issuance of its executive regulations. Therefore, compliance with and the implementation of the UAE Law will start six months after the issuance of its executive regulations.

United Kingdom

Aaron P Simpson, James Henderson and Jonathan Wright

Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The primary legal instruments include the UK's Data Protection Act 2018 (DPA 2018) and Regulation (EU) 2016/679 (the General Data Protection Regulation) as transposed into national law of the United Kingdom by the UK European Union (Withdrawal) Act 2018 and amended by the UK Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the UK GDPR).

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

DPA 2018 and the UK GDPR are supervised by the Information Commissioner's Office (ICO). The ICO may:

- seek entry to premises subject to a warrant issued by a court;
- require the provision of information by service of information notices;
- by notice, require government departments to undergo a mandatory audit (referred to as 'assessment'); and
- conduct audits of private sector organisations with the consent of the organisation.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Following the UK's exit from the European Union, the ICO no longer participates in the GDPR's 'one-stop-shop' mechanism, under which organisations with a main establishment in the European Union may primarily be regulated by the supervisory authority of the jurisdiction in which the main establishment is located (lead supervisory authority).

DPA 2018 requires the ICO, concerning third countries and international organisations, to take steps to develop cooperation mechanisms to facilitate the effective enforcement of legislation relating to the protection of PI, to provide international mutual assistance in the enforcement of legislation for the protection of PI, to engage relevant stakeholders in discussion and activities, and to promote the exchange and documentation of legislation and practice for the protection of PI.

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The ICO has several enforcement powers. Where a data controller or a data processor breaches data protection law, the ICO may:

- issue undertakings committing an organisation to a particular course of action to improve its compliance with data protection requirements;
- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps, to ensure they comply with the law; and
- issue fines of up to the greater of €17.5 million or 4 per cent of annual worldwide turnover, depending on the nature of the violation of DPA 2018 and UK GDPR.

Several breaches may lead to criminal penalties. The following may constitute criminal offences:

- making a false statement concerning an information notice validly served by the ICO;
- destroying, concealing, blocking or falsifying information to prevent the ICO from viewing or being provided with the information;
- unlawfully obtaining PI;
- knowingly or recklessly re-identifying PI that is de-identified without the consent of the data controller responsible for that PI;
- altering PI to prevent disclosure of the information in response to a data subject rights request;
- requiring an individual to make a subject access request; and
- obstructing the execution of a warrant of entry, failing to cooperate or providing false information.

Criminal offences can be prosecuted by the ICO or by or with the consent of the Director of Public Prosecutions.

1.5 Judicial review of data protection authority orders

5 Can PI owners appeal to the courts against orders of the data protection authority?

Yes. The UK GDPR gives each natural or legal person the right to an effective judicial remedy against a legally binding decision of ICO that concerns them. In addition, where an individual has lodged a complaint with the ICO, the UK GDPR and DPA 18 give the individual the right to an effective judicial remedy where the ICO does not handle the complaint or does not inform the individual within three months on the progress or outcome of the complaint.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Exemptions from the full rigour of the law apply in some circumstances and for some instances of processing. A wide exemption applies to the processing by individuals for personal and domestic use, but no sectors or institutions are outside the scope of the law. Recent European case law has clarified that this exemption applies only to purely domestic or household activities, with no connection to a professional or commercial activity. This means that if PI is only used for such things as writing to friends and family or taking pictures for personal enjoyment, such use of PI will not be subject to the UK General Data Protection Regulation (the UK GDPR).

The UK GDPR and the Data Protection Act 2018 (DPA 2018) apply to private and public sector bodies. That said, the processing of PI by competent authorities for law enforcement purposes is outside the scope of the UK GDPR (eg, the police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of DPA 2018. Also, PI processed to safeguard national security or defence is also outside the scope of the UK GDPR. However, it is covered by Part 2, Chapter 3 of DPA 2018 (the applied GDPR), which contains an exemption for national security and defence. Part 4 of DPA 2018 sets out a separate data protection regime for the intelligence services (eg, MI5, SIS (sometimes known as MI6) and GCHQ).

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Electronic marketing is specifically regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (as amended), although the UK GDPR and DPA 2018 often apply to the same activities, to the extent that they involve the processing of PI. Interception and state surveillance are covered by the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000. The interception of business communications is regulated by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

The law includes many provisions dealing with information; for example, the regulation of credit files is covered in the Consumer Credit Act 1974. Laws on e-commerce include provisions linked to the regulation of PI. Laws on defamation, copyright and computer misuse also affect data protection. However, there is no specific data protection sectoral legislation. The United Kingdom has a range of soft law instruments, such as codes of practice for medical confidentiality or the management of information held for policing, that apply in specific sectoral areas.

The DPA 2018 requires the Information Commissioner's Office (ICO) to draw up and publish codes of practice that relate to data sharing, direct marketing, age-appropriate design and data protection, and journalism. A number of these codes are not yet in force and are in the consultation phase. The ICO's Age Appropriate Design Code came into force on 2 September 2020, and following a 12-month transition period, organisations are now expected to conform to its requirements (as of 2 September 2021). In addition, the ICO's Data Sharing Code of Practice came into force on 5 October 2021. This code provides practical guidance for organisations regarding how to share PI in a manner that complies with DPA 2018 and UK GDPR.

The PECR sits alongside DPA 2018 and the UK GDPR. They give individuals specific privacy rights concerning electronic communications. In particular, the PECR sets out requirements for:

- making marketing calls, sending marketing emails and texts;
- the use of cookies (and similar technologies) on individuals' devices;
- keeping communications services secure; and
- customer privacy regarding traffic and location data, itemised billing, line identification and directory listings.

The United Kingdom has implemented the Network and Information Systems Regulations 2018 (the NIS Regulations). The UK NIS regime also includes an implementing act for digital service providers (the DSP Regulation) and specifies security requirements and incident reporting thresholds for certain organisations. While the UK GDPR concerns PI, the NIS Regulations concern the security of network and information systems. That said, there is a significant crossover between the UK GDPR and NIS Regulations, in particular owing to the UK GDPR's security requirements. In this respect, the application of the NIS Regulations is broader as it applies to digital data and not just PI.

The NIS Regulations apply to operators of essential services (OES) and relevant digital service providers (RDSPs) and are intended to address the threats posed to network and information systems. To this end, its primary focus is on cybersecurity measures. In particular, the NIS Regulations require RDSPs and OES to take appropriate and proportionate measures to manage the risks posed to the security of network and information systems.

PI formats

9 | What categories and types of PI are covered by the law?

The UK GDPR and DPA 2018 cover PI held in electronic form plus such information held in structured files, called 'relevant filing systems'. To fall within this definition, the file must be structured by reference to individuals or criteria relating to them, so that specific information about a particular individual is readily accessible.

Ultimately, whether a manual file is part of a relevant filing system is a matter of fact as well as law, and must be considered on a case-by-case basis.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Organisations that are data controllers or data processors fall within the scope of the law if they are established in the United Kingdom and process PI in the context of that establishment, or if they are not established in the United Kingdom but offer goods or services to individuals located in the United Kingdom, or monitor the behaviour of individuals located in the United Kingdom.

A data controller or data processor is 'established' in the United Kingdom if it is resident in the United Kingdom, is incorporated or formed under the laws of England and Wales, Scotland or Northern Ireland, or maintains and carries on activities through an office, branch, agency or other stable arrangements in the United Kingdom. Where a data controller or data processor is established in the United Kingdom, UK GDPR and DPA 2018 will apply regardless of whether the processing takes place in the United Kingdom or not.

Data controllers established outside the United Kingdom that are subject to the UK GDPR and DPA 2018 must nominate a representative in the United Kingdom.

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The UK GDPR and DPA 2018 apply to data controllers (ie, those who decide the purposes and the means of the data processing) and data processors (who process PI on behalf of data controllers). As such, the data controllers are the main decision makers and they exercise overall control over the purposes and means of the processing of PI. Data processors act on behalf of, and only on the instructions of, the relevant data controller.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The UK General Data Protection Regulation (the UK GDPR) requires data controllers to rely on a legal ground outlined in the UK GDPR for all processing of PI. Additional conditions must also be satisfied when processing sensitive PI.

The grounds for processing non-sensitive PI are:

- consent of the individual;
- performance of a contract to which the individual is party or to take steps at the request of the data subject before entering into a contract;
- compliance with a legal obligation, other than a contractual obligation (a legal obligation arising under the laws of a non-UK jurisdiction is not sufficient for the purposes of this ground);
- protection of the vital interests of the individual (ie, a life or death situation);
- the processing is necessary for carrying out public functions; or
- the processing is necessary for the legitimate interests of the data controller (or third parties to whom the PI is disclosed) unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

Distinct grounds for legitimate processing apply to the processing of sensitive PI (also known as 'special categories of PI'). 'Sensitive PI' is defined as PI relating to a data subject's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health;
- sex life or sexual orientation;
- genetic data;
- biometric data (when processed to uniquely identify a natural person);
- commissioning or alleged commissioning of any offence; or
- any proceedings for committed or alleged offences, the disposal of such proceedings of sentence of any court.

Where a controller processes sensitive PI it must establish a ground for processing both non-sensitive PI (eg, consent and the performance of a contract) and a separate condition for processing sensitive PI. The GDPR sets forth several conditions that may be considered in connection with the processing of sensitive PI, including:

- explicit consent of the individual;
- performance of employment law obligations;
- protection of the vital interests of the individual (ie, a life or death situation);
- 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 the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes, and that the PI is not disclosed outside that body without the consent of the data subjects;
- the processing relates to PI, which is manifestly made public by the data subject;
- the exercise of public functions;
- processing in connection with legal proceedings, legal advice or to exercise legal rights;
- processing for medical purposes;
- processing necessary for reasons of public interest in certain specific areas; or
- processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

In addition to the conditions outlined in the UK GDPR, the Data Protection Act 2018 sets forth several additional conditions that also may be relied upon, including:

- processing necessary for monitoring and ensuring equality of opportunity or treatment;
- preventing or detecting unlawful acts;
- preventing fraud;
- processing to comply with regulatory requirements relating to establishing whether a person has committed unlawful acts or has been involved in dishonesty, malpractice or other seriously improper conduct; and
- in connection with administering claims under insurance contracts or exercising rights and complying with obligations arising in connection with insurance contracts.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Data controllers are obliged to notify individuals of:

- the data controller's identity and contact information and, where applicable, the identity and contact information of its representative;
- the contact details of the data controller's data protection officer, if it has appointed one;
- the purposes for which the PI will be processed and the legal basis for processing;
- the legitimate interests pursued by the data controller, if applicable;
- the recipients or categories of recipients of the PI;

- the fact that the data controller intends to transfer the PI to a third country and the existence or absence of an adequacy decision by the European Commission, and a description of any safeguards (eg, EU model clauses) relied upon and how individuals may obtain a copy of them;
- the period for which PI will be stored or the criteria used to determine that period;
- a description of the rights available to individuals;
- the existence of the right to withdraw consent at any time;
- the right to lodge a complaint with a European Union data protection supervisory authority;
- whether the provision of PI is a statutory or contractual requirement or is necessary to enter into a contract, as well as whether the individual is obliged to provide the PI and of the consequences of failure to provide such PI; and
- the existence of automated decision-making and, if so, meaningful information about the logic involved as well as the significance and envisaged consequences of the processing for the individual.

When PI is obtained from a source other than the individual concerned, the data controller must also inform individuals of the source from which the PI originated and the categories of PI obtained.

Notice must be provided at the time the PI is collected from the data subject. When PI is obtained from a source other than the data subject it relates to, the data controller must provide the data subject with the notice:

- within a reasonable period of obtaining the PI and no later than one month;
- if the data controller uses the data to communicate with the data subject, at the latest, when the first communication takes place; or
- if the data controller envisages disclosure to someone else, at the latest, when the data controller discloses the data.

Exemptions from transparency obligations

15 | When is notice not required?

Where PI is obtained from a source other than the data subject, then provision of notice is not required if:

- the individual already has the information;
- the provision of such information would be impossible or require disproportionate effort (in which case the data controller shall take appropriate measures to protect data subjects, including making the relevant information publicly available);
- the provision of the information would render impossible or seriously impair the achievement of the objectives of the processing;
- obtaining or disclosure of the PI is required by UK law to which the data controller is subject; or
- where the PI is subject to an obligation of professional secrecy under UK law.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

The data controller must ensure that PI is relevant, accurate and, where necessary, kept up to date concerning the purpose for which it is held.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

The data controller must ensure that PI is adequate, relevant and not excessive concerning the purpose for which it is held. This means that the data controller should not collect or process unnecessary or irrelevant PI. The Data Protection Act 2018 and the UK General Data Protection Regulation do not impose any specified retention periods. PI may be held only for as long as is necessary for the purposes for which it is processed.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Yes. The UK GDPR requires PI to be retained for no longer than is necessary for the purposes for which it was originally collected. The UK GDPR does not, however, set specific time limits for different types of PI. It is the data controller's responsibility to determine how long it needs to retain PI, and this will depend on how long it needs the PI for its specified purposes. The data controller must be able to justify its chosen retention period, and it will rarely, if ever, be justifiable to retain PI on a just-in-case basis or indefinitely.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI may only be used for specified and lawful purposes, and may not be processed in any manner incompatible with those purposes. The purposes must be specified in the notice given to the individual.

In addition, recent case law has confirmed the existence of a tort of misuse of private information. Under this doctrine, the use of private information about an individual for purposes to which the individual has not consented may give rise to a separate action in tort against the data controller, independent of any action taken under the Data Protection Act 2018 or UK General Data Protection Regulation.

PI may not be processed for new purposes unless the further purposes are lawful (ie, based on a lawful ground). It may be processed for a new purpose as long as that purpose is not incompatible with the original purpose, but notice of the new purpose must be provided to the individual. Where a new purpose would be incompatible with the original purpose, it must be legitimised by the consent of the individual unless an exemption applies. For example, PI may be further processed for certain specified public interest purposes, including the prevention of crime or prosecution of offenders and processing for research, historical or statistical purposes.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Yes. The UK GDPR gives individuals the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them. The decision-making must be entirely automated and exclude any human influence on the outcome. A process will not be solely automated if a person weighs up and interprets the result of an automated decision before applying it to the individual (ie, reviews the decision and has discretion to alter it). The decision-making may, however, still be considered solely automated if a human inputs the PI to be processed and the decision-making is then carried out by an automated system. This restriction on automated decision-making applies only where the automated decision produces a legal or similarly significant effect. A decision producing a legal effect is something that affects an individual's legal status or their legal rights. This may include a decision that affects an individual's legal status under a contract (eg,

cancellation of a contract). A decision that has a similarly significant effect is something that has an equivalent impact on an individual's circumstances, behaviour or choices. For example, similarly significant effects include automatic refusal of an online credit application or e-recruiting practices without human intervention.

Where a data controller is undertaking these types of automated decisions, such decisions are only permitted where:

- the decision is necessary for the performance of a contract with the individual;
- the decision is authorised by UK law; or
- the decision is based on the individual's explicit consent.

Where the automated decision involves sensitive PI additional protections apply, and the relevant automated decision-making can only take place where:

- the individual has given his or her explicit consent; or
- the processing is necessary for reasons of substantial public interest.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Data Protection Act 2018 and the UK General Data Protection Regulation (the UK GDPR) do not specify the types of security measures that data controllers and data processors must take concerning PI. Instead, data controllers and data processors must have in place 'appropriate technical and organisational measures' to protect against 'unauthorised or unlawful processing of [PI] and against accidental loss or destruction of, or damage to, [PI]'. In addition, the UK GDPR provides several examples of security measures that data controllers and data processors should consider implementing, including:

- the pseudonymisation and encryption of PI;
- the ability to restore the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability of and access to PI promptly in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of the measures implemented.

Under the relevant provisions, in assessing what is 'appropriate' in each case, data controllers and processors should consider the nature of the PI in question and the harm that might result from its improper use, or its accidental loss or destruction. The data controller and processor must take reasonable steps to ensure the reliability of its employees.

Where a data controller uses an outsourced provider of services to process PI, it must choose a data processor providing sufficient guarantees of security, take reasonable steps to ensure that these are delivered, require the data processor to enter into a contract in writing under which the data processor will, among other things, act only on the instructions of the controller and apply equivalent security safeguards to those imposed on the data controller.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The UK GDPR requires data controllers to notify the Information Commissioner's Office (ICO) of a data breach within 72 hours of becoming aware of the breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. In addition, data controllers must notify affected individuals of a breach without undue delay if the breach is likely to result in a high risk to the rights and freedoms of affected individuals. Data processors are not required to notify data breaches to supervisory authorities or affected individuals but must notify the relevant data controller of a data breach without undue delay.

In addition to notifying breaches to the ICO and affected individuals, data controllers must also document all data breaches and retain information relating to the facts of the breach, its effects and the remedial action taken.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Yes. The UK General Data Protection Regulation (the UK GDPR) requires data controllers to be responsible for, and able to demonstrate compliance with, the UK GDPR. This requires data controllers to be proactive and organised about their approach to data protection, and be able to evidence the steps they have taken to comply with the UK GDPR. This may include, for example, implementing policies and procedures governing how PI is processed within the organisation, and ensuring staff are appropriately trained so as to ensure they are aware of their obligations when processing PI.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The UK GDPR requires data controllers and data processors to appoint a data protection officer (DPO) if:

- the core activities of the data controller or data processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the data controller or processor consist of processing sensitive PI or PI relating to criminal offences and convictions on a large scale.

If appointed, a DPO is responsible for:

- informing and advising the data controller or data processor and its employees of his or her obligations under data protection law;
- monitoring compliance with the UK GDPR, awareness-raising, staff training and audits;
- providing advice concerning data protection impact assessments;
- cooperating with the Information Commissioner's Office (ICO) and other European Union data protection supervisory authorities; and
- acting as a contact point for the ICO on issues relating to processing PI.

Organisations may also elect to appoint a DPO voluntarily; although, such an appointment will need to comply with the requirements of the UK GDPR.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Under article 30 of the UK GDPR, data controllers and data processors are required to retain internal records that describe the processing of PI that is carried out. These records must be maintained and provided to the ICO upon request.

For data controllers, the record must include the following information:

- the name and contact details of the data controller and, where applicable, the joint controller, and of the data controller's representative and DPO;
- the purposes of the processing;
- the data subjects and categories of PI processed;
- the categories of recipients to whom PI has been or will be disclosed;
- a description of any transfers of PI to third countries and the safeguards relied upon;
- the envisaged time limits for erasure of the PI; and
- a general description of the technical and organisational security measures implemented.

For data processors, the record must include the following information:

- the name and contact details of the processor and each data controller on behalf of which the processor processes PI, and of the processor's representative and DPO;
- the categories of processing carried out on behalf of each data controller;
- a description of any transfers of PI to third countries and the safeguards relied upon; and
- a general description of the technical and organisational security measures implemented.

DPA 2018 sets out several conditions for the processing of sensitive PI. To satisfy several of these conditions, data controllers must have an appropriate policy document in place. If a data controller processes sensitive PI under a condition that requires an appropriate policy document, the data controller must document the following information as part of its processing activities:

- the procedures for complying with the data protection principles in connection with the processing of the sensitive PI; and
- its policies regarding the retention and erasure of the sensitive PI, indicating how long such sensitive PI is likely to be retained.

Data controllers must review and retain the policy document when processing the relevant sensitive PI, and then for at least six months afterwards. The policy document must also be made available on request to the ICO.

Where appropriate policy documentation is required, the data controller's records of processing activities under article 30 of the UK GDPR must include:

- details of the relevant condition relied on, as set out in Parts 1 to 3 of Schedule 1 of DPA 2018;
- how processing satisfies article 6 of the UK GDPR (lawfulness of processing); and
- details of whether the sensitive PI is retained and erased following the appropriate policy documentation (and if not the reasons why not).

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Data controllers are required to carry out a data protection impact assessment (DPIA) concerning any processing of PI that is likely to result in a high risk to the rights and freedoms of natural persons. In particular, a DPIA is required in respect of any processing that involves:

- the systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing and on which decisions are made that produce legal effects concerning the natural person or that significantly affect the natural person;
- processing sensitive PI or PI relating to criminal convictions or offences on a large scale; or
- systematic monitoring of a publicly accessible area on a large scale.

A DPIA must be carried out concerning all high-risk processing activities that meet the criteria above before the processing begins. The DPIA must include at least the following:

- a systematic description of the processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- an assessment of the proportionality and necessity of the processing concerning the purposes;
- an assessment of the risks to the rights and freedoms of affected individuals; and
- information about the measures envisaged to address any risks to affected individuals (eg, safeguards and security measures).

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

The UK GDPR implements the concepts of data protection by design and data protection by default. In particular, this requires data controllers to implement appropriate technical and organisational measures in their processing systems to ensure that PI is processed under the UK GDPR, and to ensure that, by default, only PI that is necessary for each specific purpose is collected and processed. In addition, data controllers must ensure that by default PI is not made accessible to an indefinite number of persons without any intervention by the data subject.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

In the United Kingdom, data controllers are required to pay an annual registration fee to the Information Commissioner's Office (ICO). There is no obligation to do so if any of the following applies:

- no processing is carried out on a computer (or other automated equipment);
- the processing is performed solely for the maintenance of a public register;
- the data controller is a not-for-profit organisation, and the processing is only to establish or maintain membership or support of that organisation; or
- the data controller only processes PI for one or more of these purposes, and not for any other purposes:
    - staff administration;

- advertising, marketing and public relations;
- personal, family or household affairs;
- judicial functions; or
- accounts and records.

An entity that is a data processor only is not required to make this payment.

Other transparency duties

29 | Are there any other public transparency duties?

There are no additional public transparency duties.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Entities that provide outsourced processing services are typically data processors under the Data Protection Act 2018 and the UK General Data Protection Regulation (the UK GDPR). Data processors are subject to direct legal obligations under the UK GDPR in respect of the PI that they process as outsourced service providers, but nevertheless, data controllers are required to use only data processors that are capable of processing PI under the requirements of the UK GDPR. The data controller must ensure that each data processor it selects offers sufficient guarantees that the relevant PI will be processed subject to appropriate security measures and take steps to ensure that these guarantees are fulfilled. The data controller must also enter into a binding contract in writing with the data processor under which the data processor must be bound to:

- act only on the instructions of the data controller;
- ensure that persons that will process PI are subject to a confidentiality obligation;
- apply security controls and standards that meet those required by the UK GDPR;
- obtain general or specific authorisation before appointing any sub-processors, and ensure that any such sub-processors are bound by obligations equivalent to those imposed on the data processor;
- assist the data controller insofar as possible to comply with the data controller's obligation to respond to data subject rights requests;
- assist the data controller concerning the obligations to notify personal data breaches and to carry out data protection impact assessments (and any required consultation with a supervisory authority);
- at the choice of the data controller, return the PI to the data controller or delete the PI at the end of the relationship;
- notify the data controller immediately if any instruction the data controller gives infringes the UK GDPR; and
- make available to the data controller all information necessary to demonstrate compliance with these obligations, and allow the data controller (or a third party nominated by the data controller) to carry out an audit.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

It is a criminal offence to knowingly or recklessly obtain or disclose PI without the consent of the data controller or procure the disclosure of PI to another party without the consent of the data controller. This prohibition is subject to several exceptions, such as where the action was taken to prevent or detect crime. The staff of the Information Commissioner's Office (ICO) are prohibited from disclosing PI obtained in the course of their functions other than as necessary for those functions.

There are no other specific restrictions on the disclosure of PI, other than compliance with general principles and the cross-border restrictions.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The transfer of PI outside the United Kingdom is prohibited unless that country or territory ensures an adequate level of protection for the rights and freedoms of the individuals concerning the processing of their PI.

Transfers are permitted where:

- the recipient is located in a third country or territory or is an international organisation, covered by UK adequacy regulations;
- the transfer is covered by appropriate safeguards; or
- one or more of the derogations applies.

The derogations include:

- where the data controller has the individual's explicit consent to the transfer;
- the transfer is necessary to perform a contract with the data subject;
- the transfer is necessary for legal proceedings;
- the transfer is necessary to protect the vital interests of the individual;
- the transfer is necessary for the compelling legitimate interests pursued by the data controller; and
- the terms of the transfer have been approved by the ICO.

UK adequacy regulations have determined the European Economic Area and all countries, territories and international organisations covered by European Commission adequacy decisions valid as of 31 December 2020 to provide an adequate level of protection for personal data. The UK government intends to review these adequacy regulations over time.

European Commission findings have been made in respect of the use of approved standard form model clauses (standard contractual clauses) for the export of PI. Following the UK's departure from the European Union, transitional arrangements have been implemented that permit UK organisations to continue to rely on the European Commission-approved model clauses that were in place at the time of the UK's departure from the EU (that is, not including the new EU standard contractual clauses adopted in 2021) (the transitional standard clauses). The transitional standard clauses remain a valid data transfer mechanism for agreements concluded on or before 21 September 2022 and continued to provide appropriate safeguards under the UK GDPR until 21 March 2022. The ICO has published an International Data Transfer Agreement and a UK Addendum to the EU Standard Contractual Clauses. The International Data Transfer Agreement constitutes a stand-alone agreement that can be used to ensure adequacy in respect of data transfers from the UK. The UK Addendum to the EU Standard Contractual Clauses can be entered into alongside the EU standard contractual clauses and means that the EU Standard Contractual Clauses constitute adequate safeguards under UK law. The International Data Transfer Agreement and UK Addendum may be used for transfers at this point in time and must be used in respect of any new data transfers that commence on 22 September 2022 or thereafter.

Entities within a single corporate group can enter into binding corporate rules (BCRs), which must be approved by the ICO. Following the UK's departure from the European Union, new applications for UK BCRs must be submitted to the ICO using the UK BCR application forms. Organisations with existing authorised EU BCRs (ie, BCRs approved before Brexit by an EU supervisory authority) do not need to complete a

new UK BCR application. However, they must still provide the ICO with a United Kingdom version of their BCRs.

The European Commission has adopted a data protection adequacy decision relating to the United Kingdom, allowing organisations in the European Economic Area to continue to transfer personal data to organisations in the United Kingdom without restriction and without needing to rely upon data transfer mechanisms to ensure an adequate level of protection.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions on transfer apply equally to transfers to data processors and data controllers.

Onward transfers are considered in assessing whether adequate protection is provided in the receiving country. Onward transfers are covered in the transitional clauses, the International Data Transfer Agreement and in the UK Addendum to the EU Standard Contractual Clauses.

Onward transfers are not controlled specifically where a transfer is made to a country that has been the subject of an adequacy finding by the United Kingdom. It would be anticipated that the law of the recipient country would deal with the legitimacy of the onward transfer.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No. UK law does not require PI or a copy of PI to be retained within the UK.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals have the right to request access to PI that relates to them. Within one month of receipt of a valid request, the data controller must confirm that it is or is not processing the individual's PI and, if it does so, provide a description of the PI, the purposes of the processing and recipients or categories of recipients of the PI, the relevant retention period for the PI, a description of the rights available to individuals under the UK General Data Protection Regulation (GDPR) and that the individual may complain to the Information Commissioner's Office (ICO) and any information available to the data controller as to the sources of the PI, the existence of automated decision-making (including profiling), and the safeguards it provides if it transfers PI to a third country or international organisation. The data controller must also provide a copy of the PI in an intelligible form.

A data controller must be satisfied as to the identity of the individual making the request. A data controller does not have to provide third-party data unless the third party has consented to the disclosure or it is reasonable in the circumstances to disclose PI relating to the third party to the requestor.

In some cases, the data controller may withhold PI in response to a request, for example, where PI is subject to legal privilege in the UK or where disclosure of the requested PI would prejudice ongoing negotiations between the data controller and the requestor. All such exceptions are specifically delineated in the law.

In most cases, the data controller cannot charge a fee to comply with an access request. However, where the request is manifestly unfounded or excessive an organisation may charge a reasonable fee for the administrative costs of complying with the request. A reasonable fee can also be charged if an individual requests further copies of their data following a request.

Other rights

36 | Do individuals have other substantive rights?

Individuals have the following further rights:

- to rectify inaccurate PI;
- to have PI erased in certain circumstances, for example, when the PI is no longer necessary for the purposes for which it was collected by the data controller;
- to restrict the processing of PI;
- to obtain a copy of PI in a structured, commonly used and machine-readable format, and to transmit that PI to a third-party data controller without hindrance, to the extent that it is technically feasible;
- to object to the processing of PI in certain circumstances; and
- not to be subject to decisions based solely on the automated processing of PI, except in particular circumstances.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to receive compensation if the individual suffers material or non-material damage as a result of the contravention of the GDPR by a data controller or data processor. The Data Protection Act 2018 indicates that 'non-material' damage includes 'distress'. The *Lloyd v Google* decision (*Lloyd v Google LLC* [2021] UKSC 50]) has confirmed that compensation is not available for merely technical violations of UK data protection in the absence of financial loss or distress.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals may take action in the courts to enforce any of their rights.

The ICO has no power to order the payment of compensation to individuals. Therefore, an individual who seeks compensation must take action through the courts. All the other rights of individuals can be enforced by the ICO using its enforcement powers, including requiring the provision of information, and conducting audits.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

The Data Protection Act 2018 (DPA 2018), following the derogations permitted by the UK General Data Protection Regulation, provides exemptions from certain obligations, including:

- exemptions from the obligations that limit the disclosure of PI;
- exemptions from the obligations to provide notice of uses of PI;
- exemptions from reporting personal data breaches;
- exemptions from complying with the data protection principles;
- exemptions from the rights of access; and
- exemptions from dealing with other individual rights.

The grounds for exemption include exemptions to protect freedom of expression, to protect national security and policing, to support legal privilege, to protect the actions of regulatory authorities and to protect the collection of taxes and the position of the armed forces.

Exemptions also apply to protect individuals who may be vulnerable, such as those who are suffering from mental illness.

Further exemptions apply where the PI is made publicly available under other provisions.

Specific exemptions apply to allow the retention and use of PI for research. Exemptions are also available under DPA 2018 for crime, law and public protection, and finance, management and negotiations.

All exemptions are limited in scope and most apply only on a case-by-case basis.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

It is unlawful to store information (such as a cookie) on a user's device or gain access to such information unless the user is provided with clear and comprehensive information about the storage of, and access to, that information, and has provided his or her consent. Consent must be validly obtained following the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2013 (PECR). Any consent obtained must comply with the UK GDPR's standard for valid consent. Such consent is not, however, required where the information is:

- used only for the transmission of communications over electronic communications networks; or
- strictly necessary for the provision of a service requested by the user.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax telephone or other electronic channels?

It is unlawful to send unsolicited electronic marketing (ie, via technologies such as text, fax or email) unless the opt-in consent of the recipient has been obtained following the requirements of PECR. However, an unsolicited marketing email may be sent to a recipient whose contact details were obtained in the course of a sale, or negotiation of a sale, of a product or service, provided that the unsolicited marketing relates to similar products or services, the recipient is given a simple and free-of-charge means to opt out of receiving such marketing at the point their information is collected and in all subsequent marketing communications (and has not yet opted out). Any consent obtained must comply with the UK General Data Protection Regulation's (UK GDPR) standard for valid consent.

It is generally permissible to make unsolicited telephone marketing calls unless the recipient has previously notified the caller that he or she does not wish to receive such calls or the recipient's phone number is listed on the directory of subscribers that do not wish to receive such calls – the Telephone Preference Service. Any individuals may apply to have their telephone number listed in this directory. Separate requirements and separate rules around marketing to corporate subscribers (ie, an individual in his or her professional capacity) apply, and will need to be considered for business-to-business marketing.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules relating to targeted online advertising except for the general requirements under the UK GDPR and PECR. In general, consent is required for the use of cookies and similar technologies used in the context of targeted online advertising under PECR, and organisations processing PI in connection with those activities must also rely on consent as the legal basis for processing that personal data under the GDPR. The ICO has published, in draft form for public consultation, its Direct Marketing Code of Practice, which addresses various issues relating to online targeted advertising.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

The UK GDPR requires data controllers to rely on a legal ground outlined in the UK GDPR for all processing of PI. Additional conditions must also be satisfied when processing sensitive PI.

The grounds for processing non-sensitive PI are:

- consent of the individual;
- performance of a contract to which the individual is party or to take steps at the request of the data subject before entering into a contract;
- compliance with a legal obligation, other than a contractual obligation (a legal obligation arising under the laws of a non-UK jurisdiction is not sufficient for the purposes of this ground);
- protection of the vital interests of the individual (ie, a life or death situation);
- the processing is necessary for carrying out public functions; or
- the processing is necessary for the legitimate interests of the data controller (or third parties to whom the PI is disclosed) unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

Distinct grounds for legitimate processing apply to the processing of sensitive PI (also known as 'special categories of PI'). 'Sensitive PI' is defined as PI relating to a data subject's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health;
- sex life or sexual orientation;
- genetic data;
- biometric data (when processed to uniquely identify a natural person);
- commissioning or alleged commissioning of any offence; or
- any proceedings for committed or alleged offences, the disposal of such proceedings of sentence of any court.

Where a controller processes sensitive PI it must establish a ground for processing both non-sensitive PI (eg, consent and the performance of a contract) and a separate condition for processing sensitive PI. The GDPR sets forth several conditions that may be considered in connection with the processing of sensitive PI, including:

- explicit consent of the individual;
- performance of employment law obligations;
- protection of the vital interests of the individual (ie, a life or death situation);
- 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 the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes, and that the PI is not disclosed outside that body without the consent of the data subjects;
- the processing relates to PI, which is manifestly made public by the data subject;
- the exercise of public functions;
- processing in connection with legal proceedings, legal advice or to exercise legal rights;
- processing for medical purposes;
- processing necessary for reasons of public interest in certain specific areas; or
- processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

In addition to the conditions outlined in the UK GDPR, the Data Protection Act 2018 sets forth several additional conditions that also may be relied upon, including:
- processing necessary for monitoring and ensuring equality of opportunity or treatment;
- preventing or detecting unlawful acts;
- preventing fraud;
- processing to comply with regulatory requirements relating to establishing whether a person has committed unlawful acts or has been involved in dishonesty, malpractice or other seriously improper conduct; and
- in connection with administering claims under insurance contracts or exercising rights and complying with obligations arising in connection with insurance contracts.

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific rules relating to individual profiling, but the general principles and a number of obligations are likely to be relevant. For example, data controllers are required to provide notice of any profiling that is carried out, rely on an appropriate legitimate ground for processing PI and only use sensitive PI for profiling purposes with explicit consent. In addition, profiling that involves automated decision-making that produces a legal effect or a significantly similar effect on the individual may be carried out only where necessary to enter into or perform a contract between the individual and the data controller, or with the explicit consent of the data subject. As a general matter, the use of PI for profiling is likely to require the organisation to carry out a data protection impact assessment in relation to that processing.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

There are no specific rules or legislation that govern the processing of PI through cloud computing, and such processing must be compliant with the Data Protection Act 2018 (DPA 2018). The Information Commissioner's Office (ICO) has released guidance on the subject of cloud computing, which discusses the identity of data controllers and data processors in the context of cloud computing, as well as the need for written contracts, security assessments, compliance with DPA 2018 and the use of cloud providers from outside the United Kingdom. This guidance was published under the old law (ie, the Data Protection Act 1998). The ICO has confirmed that, while much of the guidance remains relevant, it intends to update the guidance in line with the UK GDPR.

HUNTON ANDREWS KURTH

Aaron P Simpson
asimpson@huntonak.com

James Henderson
jhenderson@huntonak.com

Jonathan Wright
wrightj@huntonak.com

30 St Mary Axe
London EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.huntonak.com

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In September 2021, the UK government launched a consultation on possible reforms to the UK data protection framework following the UK's departure from the EU. The stated aims of the data protection reform are to:
- support competition and innovation to drive economic growth;
- maintain high data protection standards without creating unnecessary barriers to responsible data use;
- keep pace with rapid innovation of data-intensive technologies;
- help businesses of all sizes use data responsibly without undue uncertainty or risk; and
- ensure the Information Commissioner's Office is adequately equipped to effectively regulate.

The UK government announced its proposed reform to the UK data protection framework in May 2022, and publication of a draft bill is expected later in 2022. It remains to be seen the extent to which the proposals will diverge from the data protection framework in the EU, but the UK government will need to balance the benefits of proposed reforms against the possibility of a loss of adequacy status under Regulation (EU) 2016/679 (the General Data Protection Regulation).

United States

Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The US's legislative framework for the protection of PI historically has resembled a patchwork quilt. Unlike other jurisdictions, the United States does not have a single dedicated data protection law at the federal level, but instead regulates privacy primarily by industry, on a sector-by-sector basis. There are numerous sources of privacy law in the United States, including laws and regulations developed at both the federal and state levels. These laws and regulations may be enforced by federal and state authorities, and many provide individuals with a private right to bring lawsuits against organisations they believe are violating the law. Starting in 2018, increased legislative activity at the state level signalled a shift in focus towards more broad-based consumer privacy legislation in the United States. California became the first state to enact such legislation with the passage of the California Consumer Privacy Act (CCPA), as later amended by the California Privacy Rights Act (CPRA), a broad privacy law inspired in part by the General Data Protection Regulation (GDPR) in the European Union that is aimed at protecting the personal information of consumers across industries. Since then, four other states have passed similar broad-based consumer privacy laws, all of which take effect in 2023. These new laws are the Connecticut Data Privacy Act, the Colorado Privacy Act, the Utah Consumer Privacy Act and the Virginia Consumer Data Protection Act. Moreover, as indicated above, the CCPA has been significantly amended and expanded upon by the passage of the CPRA (collectively the CCPA/CPRA), which takes effect 1 January 2023. Numerous other states have proposed similarly broad privacy legislation, while multiple comprehensive privacy bills have been introduced at the federal level in the US Congress.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

There is no single regulatory authority dedicated to overseeing data protection law in the United States. At the federal level, the regulatory authority responsible for oversight depends on the law or regulation in question. In the financial services context, for example, the Consumer Financial Protection Bureau and various financial services regulators (as well as state insurance regulators) have adopted standards under the Gramm-Leach-Bliley Act (GLB) that dictate how firms subject to their regulation may collect, use and disclose non-public personal information. Similarly, in the healthcare context, the Department of Health and Human Services is responsible for enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Outside of the regulated industries context, the Federal Trade Commission (FTC) is the primary federal privacy regulator in the United States. Section 5 of the FTC Act, which is a general consumer protection law that prohibits 'unfair or deceptive acts or practices in or affecting commerce', is the FTC's primary enforcement tool in the privacy arena. The FTC has used its authority under section 5 to bring numerous privacy enforcement actions for a wide range of alleged violations by entities whose information practices have been deemed 'deceptive' or 'unfair'. Although section 5 does not give the FTC fining authority, it does enable it to bring enforcement actions against alleged violators, and these enforcement actions typically have resulted in consent decrees that prohibit the company from future misconduct and often require audits biennially for up to 20 years. Under section 5, the FTC can fine businesses that have violated a consent order.

At the state level, attorneys general can also bring enforcement actions for unfair or deceptive trade practices, or to enforce violations of specific state privacy laws. The attorneys general in Connecticut, Colorado, Utah and Virginia are empowered to enforce violations of the respective privacy laws in those states. The California attorney general was empowered to enforce violations of the CCPA. The CPRA, which amended and expanded upon the CCPA, established the California Privacy Protection Agency (CPPA), a new regulatory body responsible for enforcing and implementing the CCPA/CPRA and imposing administrative fines for violations when the CPRA takes effect on 1 January 2023.

Apart from comprehensive state privacy laws described above, which do not contain a private right of action (except for California, where the private right of action is limited to certain actions related to data breaches), some other state privacy laws allow affected individuals to bring lawsuits to enforce violations of the law.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There are no regulations or structures that require the various federal and state data protection authorities to cooperate with one another. In the event of a data breach, however, many state attorneys general set up multistate task forces to pool resources, investigate the companies that experienced the breach, and reach a settlement or collectively litigate against the company. The resolutions often require companies to improve their information security programmes and obtain third-party assessments of their programmes.

Breaches of data protection law

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

In general, violations of federal and state privacy laws lead to civil, not criminal, penalties. The main exceptions are the laws directed at surveillance activities and computer crimes. Violations of the federal Electronic Communications Privacy Act (which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act) or the Computer Fraud and Abuse Act can lead to criminal sanctions and civil liability. Also, many states have enacted surveillance laws that include criminal sanctions, in addition to civil liability, for violations.

Outside of the surveillance context, the US Department of Justice is authorised to criminally prosecute serious HIPAA violations. In circumstances where an individual knowingly violates restrictions on obtaining and disclosing legally cognisable health information, the Department of Justice may pursue criminal sanctions.

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

The ability of an organisation to appeal orders of a regulatory authority is highly contextual and dependent on the applicable law or regulation in question. For example, in the Federal Trade Commission (FTC) context, an order is the result of an administrative proceeding before an FTC administrative law judge and the full FTC on review. An order issued by the FTC as a result of this process can be appealed directly to a federal court of appeals, where the FTC's order would be entitled to some deference on review.

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

There is no single regulatory authority dedicated to overseeing data protection law in the United States. At the federal level, different privacy requirements apply to different industry sectors and data processing activities. These laws often are narrowly tailored and address specific data uses. For those entities not subject to industry specific regulatory authority, the Federal Trade Commission (FTC) has broad enforcement authority at the federal level, and attorneys general at the state level, to bring enforcement action for unfair or deceptive trade practices in the privacy context. The comprehensive state privacy laws in California, Connecticut, Colorado, Utah and Virginia are broadly applicable but include varying exemptions for particular types of data or certain industry sectors (such as financial institutions subject to the Gramm-Leach-Bliley Act or covered entities subject to the Health Insurance Portability and Accountability Act of 1996).

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Interception of communications is regulated primarily at the federal level by the Electronic Communications Privacy Act, which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act. The federal Computer Fraud and Abuse Act also prohibits certain surveillance activities but is focused primarily on restricting other computer-related activities pertaining to hacking and computer trespass. At the state level, most states have laws that regulate the interception of communications.

There are only a handful of laws that specifically target the practice of electronic marketing and the relevant laws are specific to the marketing channel in question. Commercial email is regulated at the federal level by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). There are also state laws regulating commercial email, but these laws are generally pre-empted by CAN-SPAM. Telemarketing is regulated at the federal level by the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act, as well as regulations implemented by the FTC and the Federal Communications Commission (FCC). There are also state laws regulating telemarketing activities. Text message marketing is regulated primarily by the TCPA and regulations implemented by the FCC. Fax marketing is regulated by the TCPA, as amended by the Junk Fax Prevention Act of 2005, and state laws.

Other laws

8 | Are there any further laws or regulations that provide specific data protection rules for related areas?

In addition to the laws mentioned earlier, numerous other federal and state laws address privacy issues, including state information security laws and laws that apply to:

- consumer report information: Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act of 2003;
- children's information: Children's Online Privacy Protection Act;
- driver's information: Driver's Privacy Protection Act of 1994;
- video rental records: Video Privacy Protection Act; and
- federal government activities: Privacy Act of 1974.

The Cybersecurity Information Sharing Act (CISA) authorises entities to engage in certain cybersecurity monitoring, defence practices and information-sharing activities for purposes of protecting against cybersecurity threats. To help companies secure their information and systems, CISA provides businesses with certain liability protections in connection with monitoring information systems for cybersecurity purposes, implementing cybersecurity defensive measures, and sharing cyber intelligence with other private entities and federal government agencies.

In 2018, the California legislature enacted the California Consumer Privacy Act (CCPA), which became effective on 1 January 2020. The CCPA was amended in 2020 by the passage of the California Privacy Rights Act (CPRA) (collectively the CCPA/CPRA). The CCPA/CPRA will go into effect 1 January 2023 and will apply to any for-profit business that:

- does business in California;
- collects consumers' personal information (or on whose behalf such information is collected);
- alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information; and
- satisfies certain revenue thresholds or collects the personal information of 100,000 or more consumers or households.

Since then, four other states (Connecticut, Colorado, Utah and Virginia) have enacted similar broad-based consumer privacy laws. Like the CCPA/CPRA, these laws will apply to certain businesses that conduct business in the respective states. Unlike the CCPA/CPRA, however, the four other comprehensive state privacy laws have data processing thresholds for applicability (eg, the business must collect and process the personal information of a certain number of residents of that state on an annual basis, such as 100,000 residents annually in Virginia).

The CCPA/CPRA, the Connecticut Data Privacy Act (CTDPA), the Colorado Privacy Act (CPA), the Utah Consumer Privacy Act (UCPA) and the Virginia Consumer Data Protection Act (VCDPA) define 'personal information' broadly and contain provisions granting consumers certain rights concerning their personal information. These new laws have helped set the stage for several similar proposed laws currently pending in various state legislatures across the United States, as well as a possible federal data privacy law.

PI formats

9 | What categories and types of PI are covered by the law?

The United States does not have a dedicated data protection law. Thus, the definition of PI varies depending on the underlying law or regulation. In the state security breach notification law context, for example, the definition of PI generally includes an individual's name plus his or her Social Security number, driver's licence number or financial account number. Some states broaden the definition of PI under the data breach notification laws to include elements such as medical information, insurance information, biometrics, email addresses and passwords to online accounts. In other contexts, such as FTC enforcement actions, the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act of 1996, the definition of PI is much broader. Although certain laws apply only to electronic PI, many cover PI in any medium, including hard-copy records.

The CCPA/CPRA contains a broad definition of PI that includes any 'information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household'. The CTDPA, CPA, UCPA and VCDPA similarly contain a broad definition of PI that includes any 'information that is linked or reasonably linkable' to 'an identified or identifiable individual' or 'identified or identifiable natural person'.

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

As a general matter, the reach of US privacy laws is limited to organisations that are subject to the jurisdiction of US courts as constrained by constitutional due process considerations. Determinations regarding such jurisdiction are highly fact-specific and depend on the details of an organisation's contacts with the United States.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Generally, US privacy laws apply to all processing of PI. Until recently, with the passage of the CTDPA, CPA, UCPA and VCDPA, there have been no formal designations of 'controllers' and 'processors' under US law as there are in the laws of other jurisdictions. That being said, there are specific laws that set forth different obligations based on whether an organisation would be considered a data owner or a service provider. The most prominent example of this distinction is found in the US state breach notification laws. Pursuant to these laws, it is generally the case that the owner of the PI is responsible for notifying affected individuals of a breach, whereas a service provider is responsible for informing the data owner that it has suffered a breach affecting the data owner's data. Once a data owner has been notified of a breach by a service provider, the data owner, not the service provider, then must notify affected individuals.

The CCPA/CPRA has adopted a concept quite similar to the controller concept under the EU General Data Protection Regulation (GDPR), in that businesses directly subject to the law are defined to mean those entities who determine the purposes and means of the processing of consumers' personal information. The CTDPA, CPA, UCPA and VCDPA, also inspired in part by the GDPR, specifically use the terms 'controllers' and 'processors' to distinguish who controls or determines the purposes and means of the processing of PI and who provides PI processing services to those that control such PI.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

US privacy laws generally do not limit the processing of PI to certain specified grounds. There are, however, laws that may indirectly affect an organisation's ability to process PI. For example, organisations that are collecting personal information online from California residents must comply with the California Online Privacy Protection Act. Pursuant to this law, and general consumer expectations in the United States, the organisation must provide a privacy notice detailing the PI the company collects and how it is used. If the organisation uses the PI in materially different ways than those outlined in the privacy notice without providing notice and obtaining consent for such uses from the relevant consumers, these uses would likely be considered a deceptive trade practice under federal and state unfair competition laws. Similar laws are in place in Delaware and Nevada.

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

Since the United States does not have a dedicated data protection law, there is no singular concept of 'sensitive data' that is subject to heightened standards. There are, however, certain types of information that generally are subject to more stringent rules, which are described below.

Sensitive data under the comprehensive state privacy laws

The recently enacted Connecticut Data Privacy Act (CTDPA), Colorado Privacy Act (CPA), Utah Consumer Privacy Act (UCPA) and Virginia Consumer Data Protection Act (VCDPA), as well as the forthcoming California Privacy Rights Act, include certain obligations for businesses that process sensitive personal data. The precise definition of sensitive personal data varies under each law but, at a high level, includes data elements such as Social Security numbers, biometric or genetic data, information regarding race and ethnicity, sexual orientation data, religious beliefs and medical information. Under the California Consumer Privacy Act (CCPA), as later amended by the California Privacy Rights Act (CPRA) (collectively CCPA/CPRA), consumers will have the right to limit the use and disclosure of their sensitive personal data in certain circumstances. Under the UCPA, controllers will not be permitted to process sensitive data without first providing consumers clear notice and an opportunity to opt out of such processing. Under the CTDPA, CPA and VCDPA controllers will be required to obtain opt-in consent to process sensitive personal data.

Sensitive data in the security breach notification context

To the extent an organisation maintains individuals' names plus their Social Security numbers, driver's licence numbers or financial account numbers, notification generally is required under state and federal breach notification laws to the extent the information has been acquired or accessed by an unauthorised third party. Some states include additional data elements that could trigger breach notification. These include medical information, insurance information, biometrics, email addresses and passwords to online accounts.

Consumer report information

The Fair Credit Reporting Act (FCRA) seeks to protect the confidentiality of information bearing on the creditworthiness and standing of consumers. The FCRA limits the permissible purposes for which reports that contain such information (known as consumer reports) may be disseminated, and consumer reporting agencies must verify that anyone requesting a consumer report has a permissible purpose for receiving the report.

Background screening information

Many sources of information used in background checks are considered public records in the United States, including criminal, civil court, bankruptcy, tax lien, professional licensing, workers' compensation and driving records. The FCRA imposes restrictions on the inclusion of certain public records in background screening reports when performed by consumer reporting agencies. Employers also can investigate job applicants and employees using internet search engines, but they must comply with their legal obligations under various labour and employment laws to the extent such laws restrict the use of the information. For instance, consideration of factors such as age, race, religion, disability, or political or union affiliation in making employment decisions can be the basis for a claim of unlawful discrimination under federal or state law.

Health information

Health Insurance Portability and Accountability Act of 1996 (HIPAA) specifies permissible uses and disclosures of protected health information (PHI), mandates that HIPAA-covered entities provide individuals with a privacy notice and other rights, regulates covered entities' use of service providers (known as business associates), and sets forth extensive information security safeguards relevant to electronic PHI.

Children's information

Children's Online Privacy Protection Act (COPPA) imposes extensive obligations on organisations that collect personal information from children under 13 years of age online. COPPA's purpose is to provide parents and legal guardians greater control over the online collection, retention and disclosure of information about their children.

Under the Privacy Rights for California Minors in the Digital World law, California minors who are registered users of a website, online service or mobile application may seek the removal of content and information that the minors have posted. A 'minor' is defined as a California resident under the age of 18.

The CCPA/CPRA prohibits a business from selling a minor's personal information unless:

- the consumer is between 13 and 16 years of age and has affirmatively authorised the sale (ie, they opt in); or
- the consumer is less than 13 years of age and the consumer's parent or guardian has affirmatively authorised the sale.

The recently enacted state privacy laws in Connecticut, Colorado, Utah and Virginia similarly impose more stringent requirements with respect to the processing of personal information of children (defined as individuals under the age of 13). These laws require a business to obtain the consent of the child's parent or legal guardian prior to the processing of the child's PI, and in some cases, dependent on the jurisdiction, a data protection risk assessment may also be required.

Biometric information

Illinois, Texas and Washington have enacted biometric privacy laws that set forth requirements for businesses that collect and use biometric information for commercial purposes. These laws generally require that companies provide notice to individuals and obtain their affirmative consent before using their biometric identifiers for commercial purposes. The laws also require companies to implement security measures to protect the biometric information they maintain and to retain the biometric identifiers for no longer than necessary to comply with the law, protect against fraud, criminal activity, security threats or liability, or to provide the service for which the biometric identifier was collected.

State Social Security number laws

Numerous state laws impose obligations concerning the processing of state Social Security numbers (SSNs). These laws generally prohibit:

- intentionally communicating SSNs to the general public;
- using SSNs on identity cards required for individuals to receive goods or services;
- requiring that SSNs be used in internet transactions unless the transaction is secure or the SSN is encrypted or redacted;
- requiring an individual to use an SSN to access a website unless another authentication device is also used; and
- mailing materials with SSNs (subject to certain exceptions).

Several state laws also impose restrictions targeting specific SSN uses.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

For organisations not otherwise subject to specific regulation, the primary law requiring them to provide a privacy notice to consumers is California Online Privacy Protection Act. This law requires a notice when an organisation collects personal information from individuals in the online and mobile contexts. The law requires organisations to specify in the notice:

- the categories of PI collected through the website;
- the categories of third-party persons or entities with whom the operator may share the PI;
- the process an individual must follow to review and request changes to any of his or her PI collected online, to the extent such a process exists;
- how the operator responds to web browser 'do-not-track' signals or similar mechanisms that permit individuals to exercise choice regarding the collection of their PI online over time and across third-party websites or online services, if the operator engages in such collection;
- whether third parties collect PI about individuals' online activities over time and across different websites when an individual uses the operator's website or online service;
- the process by which consumers who visit the website or online service are notified of material changes to the privacy notice for that website; and
- the privacy notice's effective date.

Delaware and Nevada have also enacted laws that require operators of commercial internet services to provide similar information to their users when collecting PI online.

The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA) (collectively the CCPA/CPRA), also imposes specific privacy notice disclosure requirements, which apply to personal information collected both online and offline. For example, businesses must provide notice to consumers of their rights under the CCPA/CPRA (eg, the right to opt out of the sale of personal information and the sharing of personal information with third parties for cross-context behavioural advertising) and how to exercise those rights. The CCPA/CPRA also requires a business to include the following in its privacy notice:

- a list of the categories of personal information collected about consumers in the preceding 12 months;
- the categories of sources from which the personal information was collected;
- the business or commercial purpose for collecting, selling or sharing the information;
- the categories of third parties with whom the personal information is disclosed;
- lists of the categories of personal information sold or shared about consumers if the business sells consumers' personal information or shares consumers' personal information to third parties for cross-context behavioural advertising;
- a list of the categories of consumers' sensitive personal information collected or used in the preceding 12 months, including whether such information was sold or shared; and
- the length of time the business intends to retain each category of PI, including sensitive PI, or if that is not possible, the criteria used to determine the applicable retention period.

If the business sells personal information or shares personal information with a third party for cross-context behavioural advertising, it must provide a clear and conspicuous link on their website that says 'Do not sell or share my personal information' and provide consumers with a mechanism to opt out of the sale or sharing of their personal information, a decision the business must respect. Companies must update their notices at least once every 12 months. The CCPA previously imposed a limited notice obligation in the employment context and exempted the full requirements of the law with respect to personal information in this context; however, this moratorium for HR data is due to expire once the CPRA goes into effect on 1 January 2023, at which time HR data will be within the full scope of compliance obligations under the law.

The newly enacted Connecticut Data Privacy Act (CTDPA), Colorado Privacy Act (CPA), Utah Consumer Privacy Act (UCPA) and Virginia Consumer Data Protection Act (VCDPA) will similarly impose specific privacy notice disclosure requirements; however, the relevant requirements are less prescriptive than those under the CCPA/CPRA.

In addition to the state laws above, other federal laws require a privacy notice to be provided in certain circumstances, such as the following.

Children's Online Privacy Protection Act

Under the Children's Online Privacy Protection Rule of the Federal Trade Commission (FTC), implemented under the Children's Online Privacy Protection Act (COPPA), operators of websites or online services that are directed to children under 13 years old, or who knowingly collect information from children online, must provide a conspicuous privacy notice on their site. The notice must include statutorily prescribed information, such as the types of personal information collected, how the operator will use the personal information, how the operator may disclose the personal information to third parties, and details regarding a parent's ability to review the information collected about a child and opt out of further information collection and use. In most cases, an operator that collects information from children online also must send a direct notice to parents that contains the information set forth above along with a statement that informs parents the operator intends to collect the personal information from their child. The operator also must obtain verifiable parental consent before collecting, using or disclosing personal information from children.

Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), imposes several requirements on consumer reporting agencies to provide consumers with notices, including in the context of written disclosures made to consumers by a consumer reporting agency, identity theft, employment screening, pre-screened offers of credit or insurance, information sharing with affiliates, and adverse actions taken based on a consumer report.

Gramm-Leach-Bliley Act

Financial institutions must provide an initial privacy notice to customers by the time the customer relationship is established. If the financial institution shares non-public personal information with non-affiliated third parties outside of an enumerated exception, the entity must provide each relevant customer with an opportunity to opt out of the information sharing. Following this initial notice, financial institutions subject to the Gramm-Leach-Bliley Act (GLB) must provide customers with an annual notice. The annual notice is a copy of the full privacy notice and must be provided to customers each year for as long as the customer relationship persists. For 'consumers' (individuals that have obtained a financial product or service for personal, family or household purposes but do not have an ongoing, continuing relationship with the financial institution), a notice generally must be provided before the financial institution shares the individual's non-public personal information with third parties outside of an enumerated exception. A GLB privacy notice must explain what non-public personal information is collected, the types of entities with whom the information is shared, how the information is used, and how it is protected. The notice also must indicate the consumer's right to opt out of certain information sharing with non-affiliated parties. In 2009, the federal financial regulators responsible for enforcing privacy regulations implemented pursuant to GLB released model forms for financial institutions to use when developing their privacy notices. Financial institutions that use the model form in a manner consistent with the regulators' published instructions are deemed compliant with the regulation's notice requirements. In 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act transferred the GLB privacy notice rule-making authority from the financial regulatory agencies to the Consumer Financial Protection Bureau (CFPB). The CFPB then restated the GLB implementing regulations, including those pertaining to the model form, in Regulation P.

Health Insurance Portability and Accountability Act

The Privacy Rule promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires covered entities to provide individuals with a notice of privacy practices. The Rule imposes several content requirements, including:

- the covered entities' permissible uses and disclosures of protected health information (PHI);
- the individual's rights concerning the PHI and how those rights may be exercised;
- a list of the covered entity's statutorily prescribed duties concerning the PHI; and

- contact information for the individual at the covered entity responsible for addressing complaints regarding the handling of PHI.

Exemptions from transparency obligations

15 | When is notice not required?

Notice would not be required if a business is subject to specifically regulated scenarios.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

There is no existing law of general application in the United States that imposes standards related to the quality, currency and accuracy of PI. There are laws, however, in specific contexts that contain standards intended to ensure the integrity of personal information maintained by an organisation. The FCRA, for example, requires users of consumer reports to provide consumers with notices if the user will be taking an adverse action against the consumer based on information contained in a consumer report. These adverse action notices must provide the consumer with information about the consumer's right to obtain a copy of the consumer report used in making the adverse decision and to dispute the accuracy or completeness of the underlying consumer report. Similarly, under the HIPAA Security Rule, covered entities must ensure, among other things, the integrity of electronic PHI. The CCPA/CPRA, CTDPA, CPA and VCDPA grant consumers the right to correct inaccuracies in their personal information but do not expressly impost standards related to accuracy.

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Data minimisation, a core principle under the EU General Data Protection Regulation (GDPR), has historically not been mandated under US law. This principle, however, is found in recent state legislation like the CCPA/CPRA, CTDPA, CPA and VCDPA. For example, under the CCPA/CPRA, a business's collection, use, retention and sharing of consumers' PI must be reasonable necessary and proportionate to achieve the purposes for which the information was collected. The processing of PI under the CTDPA, CPA and VCDPA, similarly, must be 'reasonably necessary and proportionate' to the specified purposes provided to consumers by the businesses at collection.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

There are currently no legal requirements of general application that restrict the amount of PI that may be held or the length of time for which PI may be held; however, some statutory frameworks may impose certain retention requirements for personal information. The Safeguards Rule implemented under the Gramm-Leach-Bliley Act (GLB), for example, requires financial institutions to securely dispose of non-public personal information once such information is no longer needed for business or legal reasons, unless such information is otherwise required to be retained by law or regulation. Certain states also have laws governing data disposal; for example, Colorado requires certain persons and entities that maintain PI to create a written policy for the destruction or proper disposal of paper and electronic documents containing PI that requires the destruction of those documents when they are no longer needed.

The CCPA/CPRA prohibits businesses from retaining a consumer's personal information for longer than a period that is reasonably necessary for the stated purposes for which such information was collected. The CCPA/CPRA also requires businesses to disclose how long they intend to retain personal information, including sensitive personal information, or, if that is not possible, the criteria they use to determine the applicable retention periods.

Additionally, there are thousands of records retention laws and regulations at the federal and state level that impose specific obligations on the minimum length of time an organisation should retain records, many of which address records that contain personal information.

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Until recently, with the passage of broad-based consumer privacy laws like the CCPA/CPRA, the US has not expressly imposed restrictions on the purposes for which PI can be processed by data owners. For example, US privacy laws historically have not specifically adopted the finality principle, a core principle of data protection under the GDPR that requires controllers to only collect PI for specified, explicit and legitimate purposes and prohibits further processing of such information in a way incompatible with these previously disclosed purposes. The CCPA/CPRA prohibits businesses from collecting additional categories of personal information or processing collected personal information for additional purposes that are incompatible with the disclosed purposes for which the personal information (including sensitive PI) was collected. The CTDPA, CPA and VCDPA include similar restrictions, Under these laws, a controller must limit the collection of PI to what is 'adequate, relevant and reasonably necessary' in relation to the purposes for which such data is processed, as disclosed to the consumer. Additionally, the controller may not process PI for purposes that are 'neither reasonable necessary to, nor compatible with', the disclosed purposes for which such PI is being processed, unless the controller obtains the consumer's consent to do so.

As a practical matter, organisations typically describe their uses of personal information collected from consumers in their privacy notices. To the extent an organisation uses the personal information it collects subject to such a privacy notice for materially different purposes than those outlined in the notice, such a practice would likely be considered a deceptive trade practice under federal and state consumer protection laws.

In the United States, organisations must use the personal information they collect in a manner that is consistent with any privacy representations it has made in their privacy notices or otherwise. For example, under the CCPA/CPRA, businesses must not further process PI for any additional purpose that is not compatible with the disclosed purposes to consumers at collection, without first providing consumers a new notice. For purposes of compliance with the CCPA/CPRA, businesses must be thoughtful when drafting the required disclosers at collection, leaving some flexibility to enable the business to not only process the collected data for its current purposes but also those purposes that are reasonably anticipated in the near future.

Outside of the CCPA/CPRA context, to the extent an organisation would like to use previously collected personal information for a purpose that is materially different than the purpose represented in its privacy notice, the FTC and state attorneys general would expect the organisation to first obtain opt-in consent from the consumer for such use. Where the privacy notice is required by a statute (eg, a notice to parents under COPPA), failure to handle the PI as described pursuant to such notice also may constitute a violation of the statute.

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Certain recently enacted state privacy laws like the CCPA/CPRA, CTDPA, CPA and VCDPA provide certain restrictions with respect to the processing of PI for making automated decisions, including profiling. The CTDPA, CPA and VCPDA, for example, may require a controller to conduct a data protection risk assessment prior to the processing of PI for purposes of profiling, if certain criteria are met (eg, where such profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of or unlawful disparate impact on the consumer). The precise definition of profiling varies under each law but, at a high level, includes any form of automated processing performed on personal information to evaluate, analyse or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Additionally, the CTDPA, CPA and VCDPA provide consumers the right to opt out of the processing of PI for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. When a consumer exercise this opt-out right, businesses subject to these statutes must honour such requests.

Under the CCPA/CPRA, businesses will need to provide consumers access and opt-out rights with respect to their use of automated decision-making technology, including profiling. More specifically, businesses will be required to provide consumers 'meaningful information' about the logic involved in the decision-making processes as well as a description of the likely outcome of the process with respect to consumers. The rules detailing such requirements, however, are expected in forthcoming regulations to be issued by the new California Privacy Protection Agency.

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Similar to privacy regulation, there is no comprehensive federal information security law in the United States. Accordingly, the security obligations that are imposed on data owners and entities that process PI on their behalf depend on the regulatory context. These security obligations are set out below.

Gramm-Leach-Bliley Act

The Safeguards Rule implemented under the Gramm-Leach-Bliley Act requires financial institutions to 'develop, implement, and maintain a comprehensive information security program' that contains administrative, technical and physical safeguards designed to protect the security, confidentiality and integrity of customer information. The requirements of the Safeguards Rule apply to all non-public personal information in a financial institution's possession, including information about the institution's customers as well as customers of other financial institutions. In October 2021, the FTC significantly amended the Safeguards Rule. Previously, the Safeguards Rule was not prescriptive in nature; instead, it does set forth five key elements of a comprehensive information security programme:

- designation of one or more employees to coordinate the programme;
- conducting risk assessments;
- implementation of safeguards to address risks identified in risk assessments;
- oversight of service providers; and
- evaluation and revision of the programme in light of material changes to the financial institution's business.

The amended Safeguards Rule still affords some flexibility; however, it now includes detailed criteria that financial institutions must implement. For example, the amended rule specifies that financial institutions must implement specific safeguards including:

- encryption for all customer information in transit and at rest (subject to certain exceptions where compensating controls are implemented);
- continuous monitoring or periodic penetration testing and vulnerability assessments;
- multifactor authentication for any individual accessing an information system (or a reasonably equivalent or more secure access control approved in writing by a 'qualified individual');
- a written incident response plan; and
- steps to select and retain service providers capable of maintaining appropriate safeguards for customer information, including contractually requiring service providers to implement such safeguards, and periodically assessing service providers based on the risk they present.

Health Insurance Portability and Accountability Act

The Security Rule implemented under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to electronically protected health information (ePHI), sets forth specific steps that covered entities and their service providers must take to:

- ensure the confidentiality, integrity, and availability of ePHI;
- protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- protect against any reasonably anticipated uses or disclosures of ePHI; and
- ensure compliance with the Security Rule by the covered entity's workforce.

Unlike many other US information security laws, the Security Rule is highly prescriptive and sets forth detailed administrative, technical and physical safeguards.

State information security laws

Laws in several US states, including California, impose general information security standards on organisations that maintain personal information. California's law, for example, requires organisations that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorised access, destruction, use, modification or disclosure. Also, organisations that disclose personal information to non-affiliated third parties must contractually require those entities to maintain reasonable security procedures.

Massachusetts Standards for the Protection of Personal Information

In 2008, Massachusetts issued regulations requiring any person who holds personal information about Massachusetts residents to develop and implement a comprehensive, written information security programme to protect the data. The regulations apply in the context of both consumer and employee information and require the protection of personal data in both paper and electronic formats. Unlike the California law, the Massachusetts law contains certain specific data security standards, including required technical safeguards, on all private entities with Massachusetts consumers or employees.

New York SHIELD Act

In 2019, New York enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which amended the state's existing data breach notification law to impose certain data security requirements on businesses that own or license computerised data that includes New York residents' 'private information'. The SHIELD Act requires businesses to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, the disposal of such data. A business can comply with the SHIELD Act's 'reasonable safeguards' requirement by either being subject to and compliant with applicable federal or New York data security rules, regulations or statutes or implementing a data security programme that includes reasonable administrative, technical and physical safeguards.

New York Department of Financial Services Cybersecurity Regulation

In 2017, the New York State Department of Financial Services (NYDFS) issued a regulation that establishes a robust set of cybersecurity requirements for financial services providers regulated by the NYDFS. The cybersecurity regulation applies to entities that operate under a NYDFS licence, registration or charter pursuant to New York banking, insurance or financial services law. The cybersecurity regulation requires such covered entities to maintain a comprehensive cybersecurity programme and implement certain processes and technical controls related to risk assessments, user access privileges, software security, system auditing and monitoring, data encryption, data disposal and retention, and cybersecurity incident response. Also, the regulation assigns cybersecurity oversight responsibilities to senior officials and boards of directors and requires entities to report cybersecurity events to the NYDFS.

Nevada encryption law

Nevada law requires that organisations doing business in Nevada and that accept payment cards must comply with the Payment Card Industry Data Security Standard (PCI DSS). It requires that other organisations doing business in Nevada use encryption when transferring 'any personal information through an electronic, non-voice transmission other than a facsimile to a person outside of the secure system of the data collector', and moving 'any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor'.

State Social Security number laws

Numerous state laws impose obligations concerning the processing of state Social Security numbers (SSNs). These laws generally prohibit:

- intentionally communicating SSNs to the general public;
- using SSNs on ID cards required for individuals to receive goods or services;
- requiring that SSNs be used in internet transactions unless the transaction is secure or the SSN is encrypted or redacted;
- requiring an individual to use an SSN to access a website unless another authentication device is also used; and
- mailing materials with SSNs (subject to certain exceptions).

Several state laws also impose restrictions targeting specific SSN uses.

Key industry and government standards

There are several key industry standards in the area of information security. The PCI DSS applies to all entities that process credit or debit cards. It obliges covered entities to comply with prescriptive information security requirements, which include:

- installing and maintaining a firewall configuration to protect cardholder data;
- encrypting the transmission of cardholder data across public networks;
- protecting systems against malware and regularly updating anti-virus software or programs; and
- restricting physical access to cardholder data.

Entities subject to the PCI DSS are required to validate their compliance on an annual basis. The specific requirements necessary to certify compliance depend on the type of entity involved in the processing of payment cards and the number of payment cards processed by the covered entity pursuant to each payment card brand's compliance validation programme.

The National Institute of Standards and Technology (NIST), which is part of the US Department of Commerce, has produced various publications and guidance on a host of information security topics that are intended to help businesses. The most significant of the NIST security publications is the NIST Cybersecurity Framework. This is a flexible document that gives users the discretion to decide which aspects of network security to prioritise, what level of security to adopt and which standards, if any, to apply. Other guidance documents address methods of media sanitisation, conducting risk assessments, security considerations in the information system development life cycle and storage encryption for end-user devices.

Also, the International Organization for Standardization (ISO) is a non-governmental organisation composed of the national standards institutes of 161 countries. The ISO sets international standards across a range of industries. In the area of information security, the ISO has promulgated two important standards: 27001 and 17799/27002. ISO 27001 provides a 'process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system'. It is a flexible standard, and users are encouraged to:

- understand their information security requirements and the need to establish policy objectives for information;
- implement controls to manage information security risks in the context of the organisation's overall business risks;
- monitor and review the performance and effectiveness of the Information Security Management System; and
- continually improve the Information Security Management System based on objective measurement.

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There are no breach notification laws of general application at the federal level. There are, however, numerous targeted breach notification laws at both the state and federal level, including the following.

State breach laws

At present, all 50 states, the District of Columbia, the US Virgin Islands, Guam and Puerto Rico have enacted breach notification laws that require data owners to notify affected individuals in the event of unauthorised access to or acquisition of personal information, as that term is defined in each law. In addition to notification of individuals, a majority of the state laws also require notice to a state regulator in the event of a breach, typically the state attorney general. Although most state breach laws require notification only if there is a reasonable likelihood that the breach will result in harm to affected individuals, several jurisdictions do not employ such a harm threshold and require notification of any incident that meets their definition of a breach.

Federal interagency guidance and the Final Rule on Computer Security Incident Notification Requirements

Several federal banking regulators issued the Interagency Guidance on Response Programs for Unauthorised Access to Customer Information and Customer Notice in 2005. Entities regulated by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision are subject to the Interagency Guidance. The Interagency Guidance sets forth that subject financial institutions must develop and implement a response programme to address incidents of unauthorised access to customer information processed in systems the institutions or their service providers use to access, collect, store, use, transmit, protect, or dispose of the information. Also, the Interagency Guidance contains three key breach notification requirements. First, when a financial institution becomes aware of an incident involving unauthorised access to or use of sensitive customer information, the institution must promptly notify its primary federal regulator. Second, the institution must notify appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate attention. Third, the institution also must notify relevant customers of the incident if the institution's investigation determines that misuse of sensitive customer information has occurred or is reasonably possible. In this context, 'sensitive customer information' means a customer's name, address, or telephone number in conjunction with the customer's SSN, driver's licence number, account number, credit or debit card number, or a PIN or password that would permit access to the customer's account. Any combination of these data elements that would allow an unauthorised individual to access the customer's account also would constitute sensitive customer information. In November 2021, the Federal Reserve, the Federal Deposit Insurance Corporation and the Office of Comptroller of the Currency issued the Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and their Bank Service Providers (the Final Rule), which effectively amended the Interagency Guidance's previous requirement of 'promptly' notifying primary federal regulators. Under the Final Rule, a banking organisation must notify its primary federal regulator as soon as possible and no later than 36 hours after the banking organisation determines that a 'computer-security incident' has occurred, and such incident rises to the level of a 'notification incident' (each as defined under the Final Rule). Separately, the Final Rule also imposes certain notification requirements on bank service providers.

Health Information Technology for Economic and Clinical Health Act

The information security breach provisions in the Health Information Technology for Economic and Clinical Health Act (HITECH Act) apply in the healthcare context, governing both HIPAA-covered entities and non-HIPAA covered entities. The HITECH Act and the breach-related provisions of the Department of Health and Human Services regulations implementing the Act require HIPAA-covered entities that experience an information security breach to notify affected individuals, and service providers of HIPAA-covered entities to notify the HIPAA-covered entity following the discovery of a breach. Unlike the state breach notification laws, the obligation to notify as a result of an information security breach under the HITECH Act falls on any HIPAA covered entity that 'accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured [protected health information (PHI)]'. Any HIPAA-covered entity that processes unsecured PHI must notify affected individuals in the event of a breach, whether the covered entity owns the data or not.

INTERNAL CONTROLS

Accountability

23 | Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Data owners and entities that process PI on their behalf, depending on the regulatory context, may be required to implement internal controls to ensure accountability or to demonstrate compliance with their security obligations under the applicable law or regulation.

Data protection officer

24 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

No, the appointment of a data protection officer is not mandatory under the privacy rules of general application. Many organisations in the United States appoint a chief privacy officer (CPO), but his or her responsibilities are dictated by business need rather than legal requirements. Certain sector-specific laws do require the appointment of a CPO. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the appointment of a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. Also, several federal and state laws require that a chief information security officer or an equivalent be appointed. These laws include the Gramm-Leach-Bliley Act (GLB), HIPAA and the New York State Department of Financial Services' Cybersecurity Regulations.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

There are currently no legal requirements of general application that obligate owners of PI to maintain internal records or establish internal processes or documentation. Several statutory frameworks in the United States require organisations to develop an information security programme, which typically must contain internal processes and documentation. These include requirements imposed by the GLB, HIPAA and state information security laws. The CCPA and its implementing regulations, require businesses to maintain records of consumer rights requests made pursuant to the CCPA and how the business responded to such requests for at least 24 months. Such records must include:

- the date of the request;
- the nature of the request;
- the manner in which the request was made;
- the date of the business's response;
- the nature of the business's response; and
- the basis for the denial of the request, if applicable.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

There are no laws of general application in the United States that impose requirements on data owners or processors of PI to carry out risk assessments in relation to certain uses of personal information. There are, however, specific laws that address this issue. The E-Government Act of 2002, which is only applicable to US federal agencies, requires the completion and publication of privacy impact assessments when the

agency engages in a new collection of, or applies new technologies to, personal information.

The Connecticut Data Privacy Act (CTDPA), the Colorado Privacy Act (CPA) and the Virginia Consumer Data Protection Act (VCDPA) require data protection risk assessments prior to certain processing activities. The CTDPA and CPA, for example, specifically require data protection risk assessments prior to processing activities that present a heightened risk of harm to consumers, which include certain types of processing activities such as the processing of sensitive PI. The California Consumer Privacy Act (CCPA), as later amended by the California Privacy Rights Act (CPRA) (collectively the CCPA/CPRA), unlike the CTDPA, CPA and VCDPA, does not contain a risk assessment requirement; however, it does charge the California Privacy Protection Agency (CPPA) with issuing regulations requiring businesses whose processing of personal information presents significant risks to consumers' privacy or security to perform an annual cybersecurity audit that is 'thorough and independent' and to submit a risk assessment to the CPPA on a regular basis. Given that the CCPA/CPRA rule-making process is ongoing, it is difficult to anticipate how such audit and risk assessment requirements will eventually look.

Certain statutory frameworks in the United States, like the Gramm-Leach-Bliley Act and New York State Department of Financial Services, may require organisations to carry out risk assessments to develop and implement information security programmes to protect the security, confidentiality and integrity of personal information. The Safeguards Rule, for example, require financial institutions to base their information security programmes on periodic written risk assessments that (1) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorised disclosure, misuse, alteration, destruction or other compromise of such information; and (2) assess the sufficiency of any safeguards in place to control identified risks.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

Generally, there are no legal obligations concerning how PI processing operations must be designed, such as a 'privacy by design' approach. The Federal Trade Commission issued a report, however, that recommends that companies consider privacy by design principles during all stages of the design and development of products and services.

Although not expressly required, the data minimisation and purpose limitation requirements under the CCPA/CPRA, CTDPA, CPA and VCDPA, may have operational impacts on businesses, where taking a privacy by design approach may be effectively required to operationally accommodate such requirements.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There are no generally applicable registration requirements for data processing activities in the United States.

Other transparency duties

29 | Are there any other public transparency duties?

There are no other transparency obligations.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

As a general matter, organisations address privacy and information security concerns in their agreements with service providers that will provide outsourced processing services. There are no laws of general application in the United States that impose requirements on data owners concerning their service providers. There are, however, specific laws that address this issue, such as the following.

Health Insurance Portability and Accountability Act

Through the Privacy and Security Rules, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes significant restrictions on the disclosure of protected health information (PHI). The regulations require covered entities to enter into business associate agreements (BAA) containing statutorily mandated language before PHI may be disclosed to a service provider (business associate). For example, BAAs must, among other required elements: (1) establish the permitted and required uses and disclosures of PHI by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; and (3) require the business associate to implement appropriate safeguards to prevent unauthorised use or disclosure of PHI, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI.

Gramm-Leach-Bliley Act

Under the Privacy Rule enacted pursuant to the Gramm-Leach-Bliley Act (GLB), before disclosing consumer non-public personal information (NPI) to a service provider, a financial institution must enter into a contract with the service provider prohibiting the service provider from disclosing or using the information other than to carry out the purposes for which the information was disclosed. Under the Safeguards Rule enacted under the GLB, before allowing a service provider access to customer personal information, the financial institution must take reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards, and require the service provider by contract to implement and maintain such safeguards. The Safeguards Rule also requires financial institutions to periodically assess such service providers to confirm that they are maintaining the appropriate measures designed to safeguard customer NPI.

State information security and privacy laws

Several states impose a general information security standard on businesses that maintain personal information. These states have laws requiring companies to implement reasonable information security measures. California law and Massachusetts law require organisations that disclose personal information to service providers to include contractual obligations that those entities maintain reasonable security procedures. The California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively the CCPA/CPRA), prescribes additional content to be included in contracts with service providers. For example, among other contractual requirements, the contract must prohibit:

- the service provider from selling or sharing the PI;
- retaining, using or disclosing the PI:
  - for any purpose other than for the business purposes specified in the contract; or
  - outside the direct relationship between the service provider and business; or

- combining the PI that the service provider receives from the business with PI that it receives from or on behalf of another person or collects from its own interaction with the consumer.

The CTDPA, CPA, UCPA and VCDPA, similarly prescribe specific language in contracts with processors processing PI on behalf of controllers.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

A wide variety of laws contain disclosure restrictions targeted to specific forms of PI. For example, HIPAA and the GLB impose limitations on certain disclosures, such as requirements for consent and contracts with certain types of recipients. The CCPA/CPRA provides rights to consumers concerning a business's ability to sell their personal information to certain types of third parties or share their personal information to third parties for cross-context behavioural advertising. Similar to the CCPA/CPRA, the Connecticut Data Privacy Act, the Colorado Privacy Act, the Utah Consumer Privacy Act and the Virginia Consumer Data Protection Act provide rights to consumers to opt out of the sale of personal information to third parties and the processing of personal information for purposes of targeted advertising.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

US privacy laws do not impose restrictions on cross-border data transfers.

Further transfer

33 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

US privacy laws do not impose restrictions on cross-border data transfers.

Localisation

34 | Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

US privacy laws do not have data localisation laws requiring that PI or a copy of the PI be retained within the US.

RIGHTS OF INDIVIDUALS

Access

35 | Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

There are no laws of general application in the United States that provide individuals with a right to access the personal information about them that is held by an organisation. There are specific laws that address access rights, such as the following.

Health Insurance Portability and Accountability Act

Under the Privacy Rule enacted under the Health Insurance Portability and Accountability Act of 1996, an individual has a right to access protected health information (PHI) about the individual that is maintained by the covered entity unless the covered entity has a valid reason for denying the individual such access. Valid reasons can include the fact that the PHI is subject to restricted access under other laws, or that access to the PHI is reasonably likely to cause substantial harm to another person. A covered entity must provide the requested access to the PHI within 30 days of the request and must explain the justification for any denial of access.

California's Shine the Light Law

Under this law, organisations that collect personal information from California residents generally must either:

- provide such individuals with an opportunity to know which third parties the organisation shared California consumers' personal information with for such third parties' direct marketing purposes during the prior calendar year; or
- allow such individuals the right to opt out of most third-party sharing.

If an organisation implements the option in the first point above, it must provide California residents with a postal address, email address or freephone telephone or fax number that California residents may contact to obtain the list of relevant third parties. Organisations are required to respond only to a single request per California resident per calendar year.

Comprehensive state privacy laws

Under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively the CCPA/CPRA), California consumers have a right to request information about the PI organisations collected, shared and sold. Specifically, a consumer has a right to request that an organisation disclose:

- the categories of PI, including sensitive PI, the organisation has collected about that consumer;
- the categories of sources from which the PI is collected;
- the business or commercial purpose for collecting, selling or sharing of PI;
- the categories of third parties to whom the organisation disclosed PI;
- the specific pieces of PI, including sensitive PI, it has collected about that consumer;
- the categories of PI, including sensitive PI, it has sold about the consumer or shared about the consumer with third parties for cross-context behavioural advertising purposes and the categories of third parties to whom the PI was sold or shared; and
- the categories of PI that the organisation disclosed for a business purpose and the categories of third parties to whom the PI was disclosed for a business purpose.

The CCPA/CPRA also provides that an organisation's response to an access request must be delivered in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.

Under the Connecticut Data Privacy Act (CTDPA), Colorado Privacy Act (CPA), Utah Consumer Privacy Act (UCPA) and Virginia Consumer Data Protection Act (VCDPA), consumers may, dependent on the jurisdiction, have the right to confirm whether or not the controller is processing the consumers' personal information and access to such personal information; and obtain a copy of such information in a portable and, to the extent technically feasible, readily usable format that allows consumers to transmit the information to another controller without hindrance.

Other rights

36 | Do individuals have other substantive rights?

The CCPA/CPRA provides consumers with other rights, including the right to request that a business delete the personal information about the consumer that the business has collected from the consumer and direct any service providers to delete the consumer's personal information. There are several enumerated exceptions to this deletion requirement, such as if it is necessary to maintain the consumer's personal information to complete the transaction for which the personal information was collected or to protect against malicious, deceptive, fraudulent or illegal activity. The CCPA/CPRA also provides consumers the right to:

- correct inaccuracies in their personal information;
- opt out of the selling of their personal information or sharing of their personal information with third parties for cross-context behavioural advertising; and
- limit the use and disclosure of sensitive personal information (to the extent that such information is used by the business to infer characteristics about the consumer).

The CTDPA, CPA, UCPA and VCDPA, similarly, provide consumers with certain privacy rights. Dependent on the jurisdiction, such rights may include the right to:

- correct inaccuracies in their personal information;
- delete their personal information (dependent on which jurisdiction, the deletion right may be limited to the PI provided by consumer);
- opt out of the processing of their PI for purposes of targeted advertising;
- opt out of the sale of their PI; or
- opt out of the processing of their PI for purposes of profiling (where such profiling is in furtherance of decisions that produce legal or similarly significant effects concerning the consumers).

Also, some sector-specific laws provide other substantive rights. For example, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 provides individuals with the right to amend their PHI. If an individual requests that a covered entity amend the individual's PHI, the covered entity must do so within 60 days of the request and must explain any reasons for denying the request. The Children's Online Privacy Protection Act allows parents or legal guardians to revoke their consent and refuse the further use or collection of personal information from their child. This law also allows parents or guardians to request the deletion of their child's personal information. The Fair Credit Reporting Act (FCRA) provides individuals with the right to dispute and demand correction of information about them that is held by consumer reporting agencies.

Compensation

37 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to monetary damages for wrongful acts under common law and pursuant to most statutes that provide for a private right of action. Consumers often bring class-action lawsuits against organisations as a result of alleged privacy violations, such as statutory violations or other wrongful acts that affect them, such as information security breaches. In security breach cases, consumers often allege that the organisation was negligent in securing the consumers' personal information and that such negligence led to the security breach. As a general matter, consumers would need to establish that they suffered actual damages as a direct result of the organisation's negligence to succeed on their claim.

In the regulatory context, the ability to obtain monetary damages or compensation depends entirely on the statute in question. Under section 5 of the Federal Trade Commission Act (the FTC Act), for example, equitable relief is available first but then monetary penalties could reach US$46,5171 per violation for a breach of a consent order. Under the FCRA, in the event an organisation is wilfully non-compliant with the law, the Act provides for the recovery by aggrieved individuals of actual damages sustained or damages of 'not less than US$100 and not more than US$1,000' per violation, plus punitive damages, attorneys' fees and court costs. Negligent non-compliance may result in liability for actual damages as well as costs and attorneys' fees. Other laws, such as section 5 of the FTC Act, provide no private right of action to individuals and instead can be enforced solely by the regulator.

Enforcement

38 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

To the extent an individual obtains monetary relief as a result of illegal activity by an organisation, that relief will be obtained primarily through the judicial system. Typically, the civil penalties imposed by regulators are not paid directly to aggrieved individuals. There are, however, exceptions to this rule. For example, under the FCRA, organisations that settle claims with regulators can be asked to provide funds for consumer redress.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 | Does the law include any derogations, exclusions or limitations other than those already described?

There is no law of general application regarding privacy and information security in the United States, and thus, there are no derogations, exclusions or limitations of general application as there are in other jurisdictions. The Cybersecurity Information Sharing Act (CISA) provides companies with liability protection for cybersecurity monitoring and defence practices. For example, CISA pre-empts state law and grants liability protection to companies against any cause of action in any court for the monitoring of an information system and information to the extent the monitoring is conducted for cyber-security purposes delineated under the CISA.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

There have been numerous legislative efforts aimed at providing formal regulation for the use of cookies, particularly in the behavioural advertising context. To date, none of those legislative efforts has succeeded. The Federal Trade Commission (FTC) has issued a substantial amount of guidance in the area of online behavioural advertising, and the industry has responded with a series of self-regulatory frameworks. Although not focused directly on cookies, there have been several civil actions brought by individuals and regulatory enforcement actions brought by the FTC for practices that depend on the use of cookies, but the allegations tend to focus on laws of more general application, such as surveillance laws and section 5 of the FTC Act. At the state level, California law requires website operators to disclose how the operator responds to internet browser 'do not track' signals or other mechanisms that provide consumers with the ability to exercise choice regarding the

collection of personal information about an individual consumer's online activities over time and across a third-party website or online services if the operator engages in that collection. Also, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively the CCPA/CPRA), affords consumers certain rights concerning the sharing of personal information with third parties for purposes of cross-context behavioural advertising. The Connecticut Data Privacy Act (CTDPA), the Colorado Privacy Act (CPA), the Utah Consumer Privacy Act (UCPA) and the Virginia Consumer Data Protection Act (VCDPA) also afford consumers the rights to opt out of the processing of personal information for purposes of targeted advertising, which could bear an impact on the use of third-party cookies in many circumstances.

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

There are only a handful of laws that specifically target the practice of electronic marketing and the relevant laws are specific to the marketing channel in question. Commercial email is regulated at the federal level by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). There are also state laws regulating commercial email, but these laws are generally pre-empted by CAN-SPAM. Telemarketing is regulated at the federal level by the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act, as well as regulations implemented by the FTC and the Federal Communications Commission (FCC). There are also state laws regulating telemarketing activities. Text message marketing is regulated primarily by the TCPA and regulations implemented by the FCC. Fax marketing is regulated by the TCPA, as amended by the Junk Fax Prevention Act of 2005, and state laws.

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are currently no legal requirements of general application regarding targeted online advertising; however, there are specific laws that address the processing of personal information for such purposes.

The CCPA/CPRA provides consumers the right to opt out of the sharing of their personal information with third parties for purposes of cross-context behavioural advertising (in addition to the right to opt-out of the sale of PI previously provided under the CCPA). As provided above, the CCPA/CPRA prescribes certain notice disclosure requirements with respect to a business's processing practices, including the selling of personal information or sharing of personal information with third parties for purposes of cross-context behavioural advertising (eg, businesses must disclose the categories of PI, including sensitive PI, the business has sold or shared for cross-context behavioural advertising purposes in the past 12 months). A business also must provide a 'Do not sell or share my personal information' link on the homepage of its website so consumers may exercise such opt-out rights. Once a consumer exercise such opt-out rights, a business must honour the request.

The CTDPA, CPA, UCPA and VCDPA similarly provide consumers the right to opt out of the processing of PI for the purposes of targeted advertising. Businesses must clearly and conspicuously disclose to the consumer this opt-out right and provide details as to how the consumer may exercise such right. Once a consumer exercises the opt-out right, the business must honour the request. Under the CTDPA, CPA and VCDPA, a controller engaging in certain processing activities, including the processing of personal information for the purposes of targeted advertising, must first conduct and document a data protection risk assessment of the activity prior to processing.

In addition to the state laws above, there have been federal legislative efforts aimed at restricting targeted advertising practices (eg, prohibiting advertisers from targeting or using an advertising facilitator to target ads based on personal information that the advertiser obtained from a third party); however, to date, such efforts have not been successful.

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

Certain types of personal information may be subject to more stringent rules.

The CTDPA, CPA and VCDPA, for example, require controllers to obtain consumers' consent prior to the processing of 'sensitive PI', which, depending on the jurisdiction, may include:

- PI that reveals racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
- genetic or biometric data;
- precise geolocation data; or
- PI collected from or concerning a known child (in which case, consent must be obtained from the child's parent or lawful guardian).

For such consent to be valid, it must be 'a clear affirmative statement signifying a consumer's freely given specific, informed and unambiguous agreement'. Prior to the processing of sensitive PI, the CTDPA, CPA and VCDPA also require a controller to conduct a data protection risk assessment. The assessment must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by the safeguards that the controller can employ to reduce such risks.

Sensitive PI as defined under the UCPA contains similar data elements as described above. The UCPA, unlike the VCDPA and CPA, will not require consent prior to the processing of sensitive PI. Instead, a business must not process sensitive PI without first presenting the consumer with a clear notice and an opportunity to opt out of the processing of such information.

Sensitive PI as defined under the CCPA/CPRA also contain similar data elements as those described above. The CCPA/CPRA provides consumers a right to limit the use and disclosure of their sensitive personal information, to the extent the business processes the sensitive PI for purposes of inferring characteristics about consumers. Once a consumer exercises this right, the business must honour the request.

Profiling

44 | Are there any rules regarding individual profiling?

There are currently no legal requirements of general application regarding individual profiling; however, there are specific laws that address the processing of personal information for purposes of profiling.

The CTDPA, CPA and VCPDA, for example, provide consumers the right to opt out of the processing of PI for purposes of profiling (when profiling is in furtherance of decisions that produce legal or similarly significant effects concerning a consumer). Under the VCDPA, a controller processing PI for purposes of profiling must first conduct a data protection risk assessment if such profiling presents a reasonably foreseeable risk of:

- unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

- financial, physical, or reputational injury to consumers;
- a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers (where such intrusion would be offensive to a reasonable person); or
- other substantial injury to consumers.

Similarly, the CTDPA and CPA requires a controller to conduct a data protection risk assessment prior to the processing of PI if the processing activity presents a heightened risk of harm to a consumer. The statutes provide that processing PI for purposes of profiling presents a heightened risk of harm if the profiling presents a reasonable foreseeable risk of:

- unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- financial or physical injury to consumers;
- a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers (if the intrusion would be offensive to a reasonable person); or
- other substantial injury to consumers.

Under the CCPA/CPRA, businesses will need to provide consumers access and opt-out rights with respect to their use of automated decision-making technology, including profiling. Specifically, the businesses will be required to provide consumers with 'meaningful information' about the logic involved in the decision-making processes as well as a description of the likely outcome of the process with respect to consumers. Such rules, however, have not been provided and are expected in forthcoming regulations.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

The National Institute of Standards and Technology has issued guidelines on security and privacy in cloud computing that are directed at federal departments and agencies. The guidelines state that the cloud computing solution should be able to meet the specific privacy and security needs of the department or agency, and departments and agencies should remain accountable for the security and privacy of any data and applications maintained in the cloud. Also, the Department of Health and Human Services has issued guidance on the Health Insurance Portability and Accountability Act of 1996 and cloud computing, clarifying that covered entities and business associates must enter into business associate agreements with cloud service providers that store or process electronically protected health information (PHI) before storing records containing electronic PHI in a cloud computing facility.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In 2018, the California legislature enacted the ground-breaking California Consumer Privacy Act (CCPA), which signalled a dramatic shift in the data privacy regime in the United States. With a compliance deadline in 2020, the CCPA granted consumers several new privacy rights. For example, the CCPA granted a consumer the right, subject to certain exceptions, to:

- request that an organisation provide the consumer with access to and certain details about her personal information;
- request that an organisation delete any personal information about the consumer which the organisation has collected from the consumer; and
- direct an organisation not to sell the consumer's personal information.

As such, the CCPA required covered entities to make significant changes to their privacy programmes concerning how they collect, use and disclose personal information. Since 2018, the CCPA has been significantly amended and expanded upon by the passage of the California Privacy Rights Act (CPRA) by voter referendum on the November 2020 statewide ballot. For example, the CPRA provides consumers additional privacy rights, including the right to correct inaccuracies in his or her personal information and the right to not share his or her personal information with third parties for purposes of cross-context behavioural advertising. Moreover, the CPRA introduces certain data minimisation, retention and purpose limitation requirements.

Following in California's footsteps, four other states, Connecticut, Colorado, Utah and Virginia, have passed similar broad privacy laws: the Connecticut Data Privacy Act (CTDPA), the Colorado Privacy Act (CPA), the Utah Consumer Privacy Act (UCPA) and the Virginia Consumer Data Protection Act (VCDPA).

Several other state legislatures have privacy bills pending, many of which contain elements that can be found in the state privacy laws above. There also is potential for a federal data privacy law. Whether a federal law will pre-empt state laws such as the CCPA/CPRA, CTDPA, CPA, UCPA and VCDPA is also is a topic of debate and disagreement.

HUNTON ANDREWS KURTH

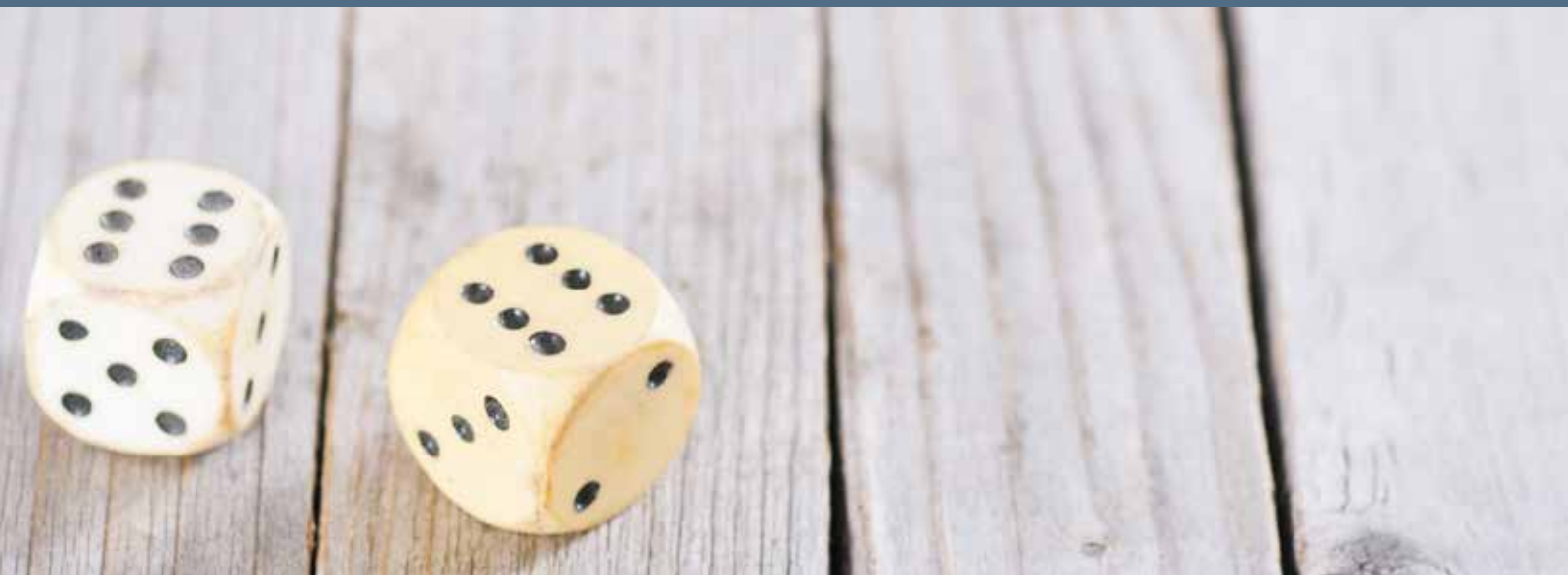
Aaron P Simpson
asimpson@huntonak.com

Lisa J Sotto
lsotto@huntonak.com

200 Park Avenue
New York City
New York
10166
United States
Tel: +1 212 309 1000
www.huntonak.com

HUNTON
ANDREWS KURTH

Leaders in Handling High-Stakes Cybersecurity Events



Luck is not a strategy.

Increase your company's resilience and responsiveness to cyber attacks.

Hunton Andrews Kurth LLP's privacy and cybersecurity practice assists global organizations in managing data through every step of the information life cycle. We help businesses prepare for and respond to cybersecurity incidents all over the world. The firm is ranked as a top law firm globally for privacy and data security.

For more information, visit www.huntonprivacyblog.com.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN XXX-X-XXXXX-XXX-X