Data Protection & Privacy

Contributing editors
Aaron P Simpson and Lisa J Sotto

2019

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2019

Contributing editors

Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2018
For further information please contact editorial@gettingthedealthrough.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2012
Seventh edition
ISBN 978-1-78915-010-0

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

CONTENTS

Preface

Data Protection & Privacy 2019

Seventh edition

Getting the Deal Through is delighted to publish the seventh edition of *Data Protection & Privacy*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

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 **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 Argentina, Colombia, Greece, Korea, Malta and Taiwan.

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.gettingthedealthrough.com.

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.

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.

GETTING THE DEAL THROUGH

London
July 2018

Introduction

Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

This introductory piece 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 this global development. 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, all of which tend to 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 (for instance, 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 law that can have a significant impact on how personal information can 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 Privacy Framework (the Framework) and the African Union Convention on Cyber Security and Personal Data Protection.

Convention 108 has 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. Morocco, Burkina Faso and Argentina have been invited to accede to Convention 108 and are expected to be the next countries to become parties. All parties to Convention 108 have passed domestic laws that implement the Convention's standards. An Additional Protocol to the Convention 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 that have the potential to be applied globally. It has arguably become the backbone of data protection laws in Europe and beyond. In April 2017, the European data protection authorities issued a resolution on the modernisation of Convention 108 to ensure consistency with the GDPR.

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 US, which has accepted the Guidelines.

Both Convention 108 and the OECD Guidelines 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 Asia-Pacific Economic Cooperation (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 the counterpart of the EU's system of binding corporate rules (BCRs) for data transfers outside of the EU. In March 2018, Singapore became the system's sixth participant, joining South Korea, Canada, Japan, Mexico and the US.

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. So far the Convention has been signed by 10 African countries, and it has been

reported that a number of African countries have drafted data protection laws based on the Convention.

European approach

For more than two decades, data protection laws have been a salient feature of European legal systems. Each EU member state has 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 follow the requirements of EU Directive 2002/58/EC on privacy and electronic communications.

The data protection laws of the EU member states, the three associated states in the European Economic Area (Iceland, Liechtenstein and Norway) and EFTA-country Switzerland broadly follow 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 transposing EU member state laws were divergent in many areas. This has led to inconsistencies, which created complexity, legal uncertainty and additional costs for businesses required to comply with, in many cases, 31 different data protection laws in Europe.

This is 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 applies from 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, which will be further discussed in this publication, is a 'game changer' and one of the most significant developments in the history of EU data protection law. The impact of the GDPR is not confined to businesses based in the EU. The new rules apply 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.

EU member states have either prepared or are preparing new data protection laws at member state level 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, almost all 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 Article 29 Working Party under the previous law). This variety of guidance and recommendations at EU and member state level is likely to trigger 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 'e-privacy' now that the GDPR has been adopted. Following the 2016 consultation, the European Commission adopted on 10 January 2017 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. At the time of drafting, it is estimated that the Regulation will be finalised by 2019, but no definitive timeline has been provided by the European Commission.

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 authority. The NIS Directive entered into force in August 2016, but member states had 21 months to transpose the NIS Directive into their national laws.

Global perspective

Moving outside Europe, the picture is more varied. From an EU perspective, the US has traditionally been 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 many of the 50 states have their own privacy laws. Contrary to the EU's omnibus law approach, the US has 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). 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, President Trump signed a Presidential Executive Order aimed at strengthening the cybersecurity of federal networks and critical infrastructure.

The US also used to be in the privileged position of having 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 United States 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. In addition, it remains to be seen whether the Privacy Shield will pass the scrutiny of the CJEU. In April 2018, the Irish High Court referred a number of questions to the CJEU, including whether the rights of EU citizens are being adequately protected by the Privacy Shield framework.

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. China adopted a comprehensive Cybersecurity Law that came into effect on 1 June 2017. The 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 practices 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 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. 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. The Malaysian data protection authority recently launched a public consultation on the rules regarding cross-border data transfers, which included an initial 'whitelist' of jurisdictions deemed adequate for overseas transfers. 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. South Korea has lived up to its reputation as having one of the most strict 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 adequate and hence allowing unrestricted transfers of personal information to South Korea. There is currently no specific data protection law in Thailand, but in April 2018, the Thai government published a revised draft of its Personal Data Protection Bill, which is general in scope and moves away from the country's sector-specific approach to privacy protection. Finally, in Taiwan amendments to the Personal Information Protection Act came into effect in March 2016. The amendments introduce, inter alia, rules for processing sensitive personal information.

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 former EU 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 EU GDPR, introducing concepts such as data portability and 72-hour breach reporting. Chile, Costa Rica, Panama and Peru have launched similar initiatives, 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 that was inspired by the GDPR. The Bill will take effect 18 months after it is published in Brazil's Federal Gazette.

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. There were initially 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. 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 is not fully in force yet but is expected to be fully effective by the end of 2018. 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. Tanzania passed its Cyber Crime Act in September 2015, and Uganda is still in

HUNTON ANDREWS KURTH

Aaron P Simpson **asimpson@HuntonAK.com**
Lisa J Sotto **lsotto@HuntonAK.com**

30 St Mary Axe
London EC3A 8EP
United Kingdom

Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.HuntonAK.com

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 on the possible impact of the GDPR on Moroccan companies.

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 EU 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 EU GDPR. The UAE's Abu Dhabi Global Market enacted similar amendments to its data protection regulations in February 2018.

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.

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.

EU overview

Aaron P Simpson and Claire François
Hunton Andrews Kurth LLP

The EU General Data Protection Regulation (GDPR) became directly applicable in all EU member states from 25 May 2018 and was expected to apply in the EEA EFTA member states (Iceland, Liechtenstein and Norway) in mid-July 2018. The GDPR replaces the EU Data Protection Directive (Directive 95/46/EC) dated 24 October 1995, and aims to establish 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 new legal framework. This provides useful guidance to businesses on how to align their existing data protection practices with the GDPR.

Impact on businesses
The GDPR largely builds on the existing core principles of EU data protection law and expands them further while introducing new concepts that address the challenges of today's data-driven economy. In addition, the GDPR launches a new governance model that increases the enforcement powers of DPAs, enhances cooperation between them and promotes a consistent application of the new rules. The most significant concepts of the GDPR affecting businesses are outlined below.

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. Many online businesses that were previously not directly required to comply with EU data protection rules are now fully affected by the GDPR.

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 handled by one DPA acting as a lead DPA. In addition to the lead DPA concept, the GDPR introduces the concept of a 'concerned' DPA to ensure that the lead DPA model will not prevent other relevant DPAs having a say in how a matter is dealt with. The GDPR also introduces a detailed cooperation and consistency mechanism, in the context of which DPAs will exchange information, conduct joint investigations and coordinate enforcement actions. In case of 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. Although DPAs have adopted tools for cooperation between them, it remains to be seen how the one-stop shop mechanism will work in practice. Businesses will have to approach the DPA they consider as their lead DPA, for example, in France, 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. The GDPR imposes shared 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 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 will have to be conducted in cases of high risk data processing. Data processors are required to assist data controllers in ensuring compliance with their accountability obligations. In addition, data controllers and data processors have to implement robust data security measures and keep internal records of their data processing activities, a system that replaces the previous requirement to register with the DPAs at member state level. 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 introduces a general data breach notification requirement applicable to all industries. Such mandatory data breach notification requirements existed in a handful of EU member states only. All data controllers now 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 high risk to the individuals' rights and freedoms. Businesses face the challenge of developing data breach response plans and taking other breach readiness measures to avoid fines and the negative publicity associated with data breaches.

Data processing agreements
The GDPR imposes minimum language that needs to be included in agreements with service providers acting as data processors. That minimum language is much more comprehensive compared to what was required under the Directive. 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), 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, and an obligation to delete or return personal data to the data controller upon termination of the services. The new requirements for data processing agreements require many businesses to review and renegotiate

existing vendor and outsourcing agreements. Some DPAs (such as the French and Spanish DPAs) have developed template clauses to help businesses ensure compliance with those requirements.

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 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 introduces requirements for data controllers to make additional arrangements to ensure they obtain, maintain and are able to demonstrate valid consent. Given the stringent consent regime in the GDPR, businesses relying on consent for their core activities should carefully review their consent practices.

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 controller's data retention practices, how individuals can obtain a copy of the data transfer mechanisms that have been implemented, and whether personal data is used for profiling purposes. 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 new transparency requirements require businesses to review their privacy notices.

Rights of individuals
The GDPR strengthens the existing rights of individuals 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 to be forgotten essentially 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. 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. Businesses need to review their existing practices for handling individuals' requests and consider how to give effect to the new 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, and applies stricter conditions for obtaining an 'adequate' status. The GDPR 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; going forward, regulators may also adopt standard contractual clauses to be approved by the European Commission, and it is now 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.

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 €20 million or 4 per cent of a company's total worldwide annual turnover, whichever is greater. 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 's and EDPB GDPR guidance
The Article 29 Working Party (WP29), composed of representatives of DPAs, has ceased to exist and has been 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;
- BCR referential for data controllers;
- BCR referential for data processors;
- adequacy referential;
- guidelines on transparency;
- guidelines on consent;
- updated working document on BCR approval procedure;
- revised BCR application form for controller BCRs;
- revised BCR application form for processor BCRs; and
- position paper on the derogations from the obligation to maintain internal records of processing activities.

With the adoption of these documents, the WP29 fulfilled the majority of its objectives set out in its 2016 and 2017 GDPR Action Plans, as part of its global implementation strategy of the GDPR.

The EDPB also adopted during its first plenary meeting the GDPR guidelines on certification and those on derogations applicable to international data transfers. The EDPB will continue the work of the WP29 and provide interpretation on further aspects of the GDPR, such as its territorial scope and codes of conduct.

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 introduce or maintain 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 of 30 June 2017, for example, requires businesses to appoint a DPO if they permanently engage at least 10 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 June 21, 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. This limit is lowered to the age of 13, for example, in the UK Data Protection Act 2018 and the age of 14 in the Austrian Data Protection Amendment Act 2018 (Datenschutz-Anpassungsgesetz 2018). At the time of writing, not all EU member states 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 sum, it is fair to say that the GDPR sets the stage for a more robust and mature data protection framework in the EU for the foreseeable future, while EU member state laws complement that framework. The new rules affect virtually any business dealing with personal data relating to individuals in the EU. Businesses should be prepared for the new challenges and at the very least be able to demonstrate that they have engaged in a GDPR compliance programme, in light of the DPA inspections that are expected to be carried out in the coming months.

Aaron P Simpson **asimpson@HuntonAK.com**
Claire François **cfrancois@HuntonAK.com**

30 St Mary Axe
London EC3A 8EP
United Kingdom

Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.HuntonAK.com

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 (0)2 643 58 00
Fax: +32 (0)2 643 58 22

The Privacy Shield

Aaron P Simpson
Hunton Andrews Kurth LLP

Twenty-first century commerce depends on the unencumbered flow of data around the globe. At the same time, however, individuals everywhere are clamouring for governments to do more to safeguard their personal data. A prominent outgrowth of this global cacophony has been reinvigorated regulatory focus on cross-border data transfers. Russia made headlines because it enacted a law in September 2015 that requires companies to store the personal data of Russians on servers in Russia. While this is an extreme example of 'data localisation', the Russian law 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 EU to the US for nearly 15 years, was invalidated by the Court of Justice of the European Union (CJEU) in October 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 in Europe. In January 2017, the Swiss government announced its approval of a Swiss–US Privacy Shield framework.

Contrasting approaches to privacy regulation in the EU and US

Privacy regulation tends to differ from country to country around the world, 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 EU and the US, which are literally and figuratively an ocean apart. Policymakers in the EU and the US 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 EU and the US. With the onset of the Privacy Shield, policymakers have again sought to bridge the gap between the different regulatory approaches in the EU and US.

The European 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 takes an understandably hard-line approach to data protection. The processing of personal data about individuals in the EU is strictly regulated on a pan-EU basis by the General Data Protection Regulation (GDPR), which entered into force on 25 May 2018. Unlike its predecessor, the Data Protection Directive 95/46/EC, the GDPR is not implemented differently at the member state level but instead applies directly across the EU as a Regulation.

Extraterritorial considerations are an important component of the data protection regulatory scheme in Europe, as policymakers have no interest in allowing companies to circumvent European data protection regulations simply by transferring personal data outside of Europe. These extraterritorial restrictions are triggered when personal data is exported from Europe 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 Europe, and for its own cultural and historical reasons, the US does not maintain a singular, comprehensive data protection law regulating the processing of personal data. Instead, the US favours a sectoral approach to privacy regulation. As a result, in the US there are numerous privacy laws that 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 regulators are subject to general consumer protection regulation at the federal and state level. Making matters more complicated, common law in the US 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 1990s internet boom, the differences in the regulatory approaches favoured in Europe versus the US became a significant issue for global commerce. Massive data flows between Europe and the US were (and continue to be) relied upon by multinationals, and European 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 Europe to the US made pursuant to the accord were considered adequate under European law. Previously, in order to achieve the adequacy protection provided by the framework, data importers in the US were required to make specific and actionable public representations regarding the processing of personal data they imported from Europe. 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, 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 to the extent their certification materially misrepresented any aspect of their processing of personal data imported from Europe.

Since its inception, Safe Harbor was popular with a wide variety of US companies whose operations involved the importing of personal data from Europe. While many of the companies that certified to the framework in the US did so to facilitate intra-company transfers of employee and customer data from Europe to the US, 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 US, 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 Europe and, ultimately, was invalidated in October 2015.

Invalidation of the Safe Harbor framework

Criticism of the Safe Harbor framework from Europe began in earnest in 2010. In large part, the criticism stems from the perception that the Safe Harbor was too permissive of third-party access to personal data in the US, 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 US 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 Europe. 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 Europe 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 EU.

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 US and more clarity regarding US government access to personal data exported from the EU under the Safe Harbor framework.

In October 2013, Safe Harbor was invalided 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 US. 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 future of 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 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. After certification, entities certified to the Privacy Shield may import personal data from the European Union without the need for another cross-border data transfer mechanism, such as standard contractual clauses. The privacy principles in the Privacy Shield are substantively comparable to those in Safe Harbor but are more robust and more explicit with respect to the actions an organisation must take in order 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 Europe (including the Article 29 Working Party (the Working Party), 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 Europe. Based on this feedback, the revised Privacy Shield framework was released in July 2016 and formally approved in the European Union. In addition, the Working Party, which is the group of European Union member state data protection authorities, subsequently offered its support, albeit tepid, for the new framework.

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 with respect to government access requests for national security reasons, and how Privacy Shield-certified entities have sought to comply with their Privacy Shield obligations. In November 2017, the Working Party adopted an opinion on the review. The opinion noted that the Working Party '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 with respect to both the commercial and national security aspects of the Privacy Shield framework. The opinion indicated that, if the EU and US do not, within specified time-frames, adequately address the Working Party's concerns about the Privacy Shield, the Working Party may 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. With respect to the Privacy Shield's commercial aspects, the 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;

HUNTON ANDREWS KURTH

Aaron P Simpson **asimpson@HuntonAK.com**

30 St Mary Axe
London EC3A 8EP
United Kingdom

Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.HuntonAK.com

- strengthened enforcement through continued oversight by the Federal Trade Commission, 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.

With respect to 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 re-issuing of Intelligence Community Directive 107;
- independent oversight through the nomination of three individuals to the Privacy and Civil Liberties Oversight Board (PCLOB) with the aim of restoring 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 in relation to the transfer of their data to the US; and
- US legal developments take into account the Privacy Shield, such as Congress's reauthorisation of the Foreign Intelligence Surveillance Act's Section 702 (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 (LIBE) Committee of the European Parliament voted on a resolution to recommend that the European Commission suspend the Privacy Shield unless the US complied fully with the framework by 1 September 2018. This resolution is a non-binding recommendation, and the full European Parliament was due to vote on the resolution in July 2018. While the results of that full vote could impose additional pressure on the European Commission to take action with respect to the Privacy Shield, it also does not bind the European Commission with respect to the Privacy Shield framework.

Argentina

Diego Fernández
Marval, O'Farrell & Mairal

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

In Argentina, the most comprehensive statutory regulation regarding the protection of personal data is the Data Protection Law No. 25,326 (the DPL), which is regulated by Decree No. 1558/2001 and enforced by the Data Protection Authority (the DPA). The legal framework also includes the complementary regulations issued by the DPA. The DPL applies to personal data of both individuals and legal entities that is stored in public and private files, records, databases and other means of electronic record-keeping aimed at providing reports.

The DPL is based on rights acknowledged in section 43 of the Argentine Constitution, which guarantees the right to habeas data. The DPL was inspired by EU Directive 95/46/CE and the Spanish Data Protection Law.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The authority responsible for overseeing the DPL is referred to generically as the DPA. The current agency acting as Argentina's DPA is the Agency of Access to Public Information, which replaced the National Directorate of Personal Data Protection through the adoption of Decree No. 746/2017. The agency is an autarchic entity that operates with functional autonomy under the President's Chief of Staff Office. Under Law No. 27,275, the agency has the duty of supervising the protection of personal data in order to guarantee the rights of good reputation, privacy and access to one's personal data. It is also afforded the powers to receive and handle complaints filed by data subjects, request public and private entities to provide information on the processing of personal data, approve international data transfer agreements submitted by interested parties and conduct inspections to check compliance with the DPL.

3 Legal obligations of data protection authority

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

The DPL does not contain any provisions that require the DPA to cooperate with the data protection authorities of other countries or establish mechanisms to resolve different approaches.

4 Breaches of data protection

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

Breaches of the DPL may lead to administrative sanctions, civil proceedings or criminal penalties. The DPA may apply the following administrative penalties in the event of violation of the DPL:

- observation;
- suspension;
- fines of between 1,000 and 100,000 pesos;
- business closure; or
- cancellation of the file, record or database.

Depending on the type of infringement, the range of administrative sanctions and fines is as follows:

- moderate infringement: fine of 1,000 to 25,000 pesos;
- severe infringement: suspension of one to 30 days or a fine of 80,001 to 100,000 pesos, or both;
- very severe infringement: suspension of 31 to 365 days or a fine of 80,001 to 100,000 pesos, or both.

DPA Rule No. 71 E/2016 capped fines applicable for various infringements encompassed by the same administrative proceeding. In the same administrative proceeding, such fines may not exceed 1,000,000 pesos for moderate infringements, 3,000,000 pesos for severe infringements and 5,000,000 pesos for very severe infringements.

Moreover, data subjects may bring civil proceedings seeking damages in connection with the unauthorised processing of their personal data. In addition, sections 117bis and 157bis of the Criminal Code punish with one month to three years of imprisonment those who:

- illegally insert false information in a database;
- knowingly supply false information stored in a database to a third party;
- knowingly and illegally gain access to a database containing personal data in violation of its security systems;
- disclose personal data protected by duty of confidentiality pursuant to law; or
- illegally insert data in a database.

Scope

5 Exempt sectors and institutions

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

The DPL covers both the public and private sectors in general. In particular, section 43 of the Argentine Constitution and the DPL expressly state that the secret nature of journalistic information should not be impaired. At the same time, the DPL provides certain exceptions when it comes to national security and the public interest. The DPL also does not apply to processing personal data in the framework of opinion polls, surveys, statistical or census works conducted by the authorities, market research or scientific or medical research, to the extent that the data collected cannot be attributed to an identified or identifiable individual or legal entity. The DPL further does not apply to the processing of personal data by an individual in the course of household activity.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The DPL does not contain provisions regarding the interception of electronic communications. However, section 153 of the Argentine Criminal Code contains provisions on interception. It provides for periods of imprisonment from 15 days to six months for those found guilty of intercepting communications. Passing on or publication of the contents of the intercepted electronic communication is punishable by additional sentences ranging from one month to one year of imprisonment.

In connection with marketing communications, section 27 of the DPL provides that personal data may be used to determine consumer profiles for marketing purposes, provided that such data is gathered from sources accessible to the public or the data subject voluntarily provided the information or consented to its use. On the other hand, Decree No. 1158/01 allows for the collection, processing and assignment of personal data for marketing purposes without the consent of the data subject as long as the data subject is identified only by their belonging to groups based on their preferences or behaviour and the personal data is limited to that which the marketer needs to make an offer. Since there is some disagreement as to how the provisions of the DPL and Decree No. 1158/01 relate to one another and whether they are in conflict or not, a conservative approach would be to rely on opt-in consent for marketing communications.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

In the case of databases created for the purpose of supplying credit information, the relevant financial information of an individual or legal entity may be stored and disclosed for a period of five years, or two years in the case of information regarding defaults that have been resolved.

Argentina lacks specific regulation on data protection in connection with employment issues. However, Labour Contract Law No. 20,744 includes some limits and conditions to employers' powers of employee organisation and direction that are applicable to data protection. Employers must exercise organisation and direction powers in a functional manner, taking into account their employees' personal and property rights and treating their information with the highest degree of caution and confidence in order to avoid affecting the employees' dignity and privacy.

Prevailing case law has generally upheld the employer's right to monitor its employees' corporate or work emails, as long as they have provided their prior and informed consent. Decisions on the matter (mainly from labour courts) have considered that a corporate email account is a work tool which may be controlled and monitored by the employer, subject to certain conditions (eg, the existence of a policy notified in writing to the employee, informing them that the corporate email is a business tool, that the employee should have no expectation of privacy – even after he or she has created a password – and reserving the right to monitor the information). For example, in 2003 the National Court of Appeals in Labour Matters, Courtroom VII, considered that if a company does not have a clear policy on the use of this tool, it could create a false expectation of privacy.

8 PII formats

What forms of PII are covered by the law?

The DPL covers all types of personal data with no limit as to the format in which it is stored. Personal data includes information referring to identified or identifiable natural and legal persons, meaning that dissociated personal information is not covered by the DPL.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The DPL does not clearly distinguish whether its application is restricted to local databases or also covers databases located outside Argentina that contain the personal data of Argentine and foreign data subjects. Thus, if personal data is stored in a database located outside of Argentina and managed or owned by a foreign entity, it could be argued that the DPL does not apply and that local authorities have no jurisdiction. However, there have been no regulations or judicial precedents to clarify this matter yet.

10 Covered uses of PII

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

The DPL has a wide definition of data processing, which covers all processing activities in general, including the collection, preservation, organisation, storage, modification, analysis, blocking, transfer and destruction of personal data.

In addition, the DPL distinguishes between data controllers and providers of data processing services. It defines a data controller as the individual or legal entity that owns a database. Although the DPL does not include a definition of data processing service providers, it does contain a provision aimed specifically at regulating them. Section 25 of the DPL refers to the general requirements of data processing services and to the duties of service providers (see question 32).

Legitimate processing of PII

11 Legitimate processing – grounds

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

The general principle under the DPL is that any processing of personal data (including any disclosure, collection, storage, amendment and destruction) must be specifically consented to by the data subject. Such consent must be prior, given freely, based upon the information previously provided to the data subject (informed) and expressed in writing or by equivalent means, depending on each case. The data subject may revoke the consent at any time, although this will not have a retroactive effect.

No consent is needed for certain data processing, occurring when the personal data:

- is obtained from public sources with unrestricted access;
- comprises the following categories of data: name, ID number, tax or social security number, occupation, date of birth or domicile;
- derives from a contractual, scientific or professional relationship with the data subject, provided that the data is necessary for the development of and compliance with the relationship; or
- is related to transactions made by financial institutions and information received by their own clients.

Further, the national government is allowed to process personal data without prior consent where national defence, public security or the prosecution of criminal offences is involved.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The DPL provides for a more restrictive set of regulations for sensitive data. Sensitive data refers to any personal data revealing racial or ethnic origin, political affiliation, religious, moral or philosophical convictions, union activity or information related to health or sexual orientation.

As a general rule, sensitive data may only be collected where authorised by law and for a public interest purpose. Sensitive data requires the data subject's consent for any processing, and no data subject is obliged to supply such information. However, sensitive data may be collected for statistical or scientific reasons as long as data subjects cannot be identified. Health institutions and practitioners are also entitled to collect sensitive information on health, as long as it is connected to the physical or mental health of patients.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Any processing of personal data must be specifically consented to by the data subject. As part of this consent, the data subject must be informed about:

- the purpose of the personal data collection and information regarding potential recipients of the information;
- the existence of the database and the identity and domicile of the data processor;
- whether the questions to be answered by the data subject when information is gathered are optional or compulsory;
- the consequences arising from the supply, failure to supply or inaccurate supply of information; and
- the possibility of the data subject exercising their right to access, rectify or remove personal data stored in the database.

Such information shall be provided when the personal data is obtained and must be expressly and clearly provided.

14 Exemption from notification

When is notice not required?

Consent is not required in certain limited cases (see question 11).

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The DPL requires that personal data be stored so that the data subject can exercise the rights of access, rectification, cancellation and opposition. Data subjects may revoke the consent at any time, with no retroactive effects.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The DPL requires that collected personal data be accurate and updated if necessary. Personal data that is totally or partially inaccurate or incomplete must be deleted, substituted or completed by the data controller when the data controller knows of such inaccuracy or incompleteness.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The DPL does not restrict the amount of information that can be held, although it does impose different regulations and registration requirements based on how much information is held. Personal data may be held for as long as it is necessary or current for the purposes for which it was collected, after which it must be destroyed or deleted.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The DPL requires that collected personal data be used only for purposes compatible with those for which the data was collected. Any use beyond that is forbidden.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The general principle under the DPL is that any processing of personal data must be specifically consented to by the data subject. Therefore, a data subject must consent in order for personal data to be used for a new purpose.

Security

20 Security obligations

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

The DPL states that the data controller and the user of a database containing personal data must adopt the necessary technical and organisational measures to guarantee the protection and confidentiality of the data, in order to prevent any adulteration, loss or unauthorised access or processing. Moreover, DPL Rule 11/2006 establishes three levels of mandatory security measures based on the nature of data to be protected: basic, medium and critical.

The basic security level applies to all databases. Databases under this security level must implement and update a security document containing, among others, the following information:

- employee functions and obligations;
- descriptions of files containing personal data and the systems used to store and treat them;
- descriptions of control procedures;
- descriptions of security incident notifications, management and responses;
- procedures to make backup copies and recover data;
- updated information on authorised users;
- procedures to identify and authenticate authorised users;
- user access control;
- measures to protect against malicious software; and
- procedures to guarantee proper database management.

The medium security level applies to databases owned by companies that render public services and databases owned by public and private entities that must observe legally provided duties of confidentiality. Databases under this security level must follow the measures required by the basic security level, as well as:

- appoint an IT security person or team;
- perform periodical data security audits;
- restrict access attempts for systems containing information;
- control physical access to places where systems are stored;
- implement a registry of logs for systems containing information;
- implement required measures to prevent the recovery of previously deleted or erased information;
- implement a backup or information recovery protocol; and
- only perform system tests on real files and data when proper security measures are implemented.

The critical security level applies to databases that store sensitive personal data, except for those that have to process such data for administrative purposes or by legal order. Databases under this security level must abide by basic and medium security level requirements as well. In addition, critical security databases must do the following:

- encrypt devices used to store personal data;
- implement a registry containing detailed information about each access and relevant authorisations, to be kept for three years;
- keep additional backups off premises and under strict security measures; and
- adopt encryption when transferring data.

21 Notification of data breach

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 DPL does not impose a general duty to notify either individuals or the DPA of a data breach.

However, the Argentine Civil and Commercial Code contains a general obligation to prevent damages, including damages caused by a third party. In particular, section 1710 provides that all individuals must adopt, in good faith and as required by the particular circumstances of the case, reasonable measures to prevent or mitigate damage caused by a third party. In this regard, in some circumstances this

obligation could be construed as requiring the notification of a data breach when doing so would help prevent any harm to a third party. Moreover, it is worth mentioning that a recent draft bill presented by the DPA includes mandatory notification in the event of a data breach (see 'Update and trends').

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

There is no general duty under the DPL to appoint a data protection officer. However, organisations under the medium and critical security levels must appoint a head of data security. The head of data security is in charge of the security measures to be applied to the database.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Data controllers must abide by the DPL's security levels, which impose various requirements for record-keeping and internal documentation and procedures.

24 New processing regulations

Are there any obligations in relation to new processing operations?

There are no regulations on new processing operations, such as requirements to carry out privacy impact assessments or apply a privacy-by-design approach, in the DPL. However, DPA Rule No. 18/2005, which established guidelines of good practices in the process of mobile app development, does recommend developing applications using a privacy-by-design approach that entails considering any privacy and data protection implications since day one, and also 'privacy by default'.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

Database registration is required for all data controllers to legally collect, store and process personal data. Registration must be completed before any personal data processing begins. The DPA has also implemented a simplified registration process available to insurance brokers and members of associations with a code of conduct approved by the DPA.

26 Formalities

What are the formalities for registration?

Registration consists of completing a form, submitting proper documentation and paying an annual fee. The form consists of the following information:

- name and domicile of the data controller;
- nature and purpose of the database;
- category of personal data collected and stored;
- means by which personal data is collected and stored;
- the purpose of the data collection and the names of the individuals or entities to which data may be revealed;
- countries to which data may be transferred;
- security measures to be implemented;
- period for which the data is to be retained; and
- terms and conditions under which data subjects may access their information.

The form may be submitted online, but a hard copy must still be sent to the DPA. Registration is valid for one year. Requests for renewal must be filed with the DPA at least 45 days before the registration's expiration. The registration fee varies between 300 and 3,000 pesos, depending on the number of individuals or entities included in the database. There are no fees for registration or renewal requirements for databases of fewer than 5,000 individuals or entities, as long as the database does not include sensitive data.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Failure to renew an existing registration is considered a moderate infringement of data protection regulations and may be subject to fines of 1,000 to 25,000 pesos. Failing to register a database is considered a severe infringement of data protection regulations and may be subject to fines of 25,000 to 80,000 pesos or suspension of one to 30 days, or both. Failing to register a database after being requested to do so by the DPA is considered a very severe infringement and may be subject to fines of 80,001 to 100,000 pesos or suspension of 31 to 365 days, or both.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

When registration applications require amendment to comply with regulations, the DPA will notify the data controller of such amendments, which must be submitted before registration is approved. However, the DPA has not established grounds for outright refusal.

29 Public access

Is the register publicly available? How can it be accessed?

Yes, the register is publicly available and can be accessed through the DPA's website.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Being registered allows databases to be in compliance with the DPL, which imposes certain requirements but also shields the database from fines related to non-registration.

31 Other transparency duties

Are there any other public transparency duties?

The DPL does not contain any further public transparency duties.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Entities that provide outsourced processing services are considered data processors. In that case, the DPL requires a data processing agreement between the data processor and data controller. Decree No. 1558/2001 provides that the agreement must:

- detail the security measures mandated by the DPL;
- include the parties' confidentiality obligations;
- establish that the data processor will only act as instructed by the data controller; and
- establish that the data processor is also bound by the DPL's data security requirements.

The data may only be used for the purpose outlined in the agreement, and may not be assigned. After the data processing has been rendered, the data must be destroyed, except in the case of express authorisation to the contrary from the data controller, when it can be reasonably assumed that additional services will be required. The data can then be stored for a maximum of two years.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosure to other recipients can only be made when the data subject has consented to the disclosure.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The DPL prohibits the transnational transfer of personal data from Argentina to other countries or to international organisations if the countries or organisations do not provide an adequate level of data protection. Transfers may be done when the data subject consents to the transfer or when the adequate protections arise from contractual clauses or self-regulated systems. This requirement does not apply to international judicial collaborations, certain cases regarding medical treatments, banking or stock exchange transfers conducted in accordance with applicable laws and regulations, personal data transfers under international treaties or transfer between government intelligence agencies for the purpose of fighting organised crime, terrorism or drug dealing.

DPA Rule No. 60-E/2016 (Rule 60) provides a list of jurisdictions which the DPA considers provide an adequate level of protection. These are the member states of the European Union and the European Economic Area, Switzerland, Guernsey and Jersey, the Isle of Man, the Faeroe Islands, Canada (only applicable to the private sector), New Zealand, Andorra and Uruguay. In some non-binding administrative decisions, the DPA has found the United States not to meet an adequate level of protection.

Moreover, Rule 60 approved two sets of standard model clauses addressing the two most common types of transfer of data: the assignment of data to a third party and the transfer of data for the rendering of data processing services. The use of these standard model clauses is mandatory for the transfer of data to countries that do not meet an adequate level of protection, provided that the data subject has not provided express consent or that a self-regulatory mechanism with adequate protection is not in place. If the parties choose to use a model different from the ones indicated by the DPA or one that does not include the principles, warranties and content covered by the approved standard model clauses, they are required to submit the agreement for DPA approval within 30 calendar days from the execution date.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

When a data controller registers a database with the DPA, it must provide a list of the countries to which data is likely to be transferred. No additional notification or authorisation is required.

36 Further transfer

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

Yes, they do.

Rights of individuals

37 Access

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

Data subjects possess a number of rights under the DPL regarding databases and their accompanying registries, including the right to access any database containing their personal information. The right of access includes the right for data subjects to:

- know whether their personal data is in the database;
- know all of their information in the database;
- request information on the data's source;
- request information on the data collection's purpose;
- know the intended use of their personal data; and
- know whether the database is registered in accordance with the DPL's requirements.

38 Other rights

Do individuals have other substantive rights?

Data subjects have the following additional rights:

- to request information in connection with their data; and
- to request the correction, deletion, update or confidential processing of their data.

39 Compensation

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 claim damages under general civil law principles contained in the Civil and Commercial Code if they are affected by breaches of the DPL. In order to obtain compensation, the data subject would have to prove effective damages as a result of the breach, and establish a causation relationship with the data controller.

40 Enforcement

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

Both. The infringement of the DPL can be reported to the DPA, which is entitled to enforce the provisions of the DPL (it can impose fines and sanctions but does not have the authority to award damages or costs). It can also serve as basis for a civil action before the courts. In some cases, infringement of the DPL could constitute a crime to be pursued before the criminal courts.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No, it does not.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Based on the general principles of Administrative Procedural Law, the DPA's decisions must be first challenged before the administrative authorities. Thereafter, decisions can be appealed before the courts.

Update and trends

In June 2016, the DPA issued a press release on the need to rethink the DPL. Although not binding, the DPA made public a draft of a bill intended to supersede the current DPL. The draft bill includes several relevant aspects. Among other things, it:

- limits the concept of data subject to natural persons and excludes legal entities;
- revisits general concepts included in the current DPL, such as databases, personal data and sensitive data, and it incorporates new ones;
- includes accountability obligations and eliminates the requirement of registering databases with the DPA;
- establishes that the legal basis for the processing of personal data is still the data subject's express consent, although under specific circumstances consent can be given implicitly, with the addition of the data processor's legitimate interest as a new legal basis;
- expressly acknowledges the right to be forgotten and the right to data portability;
- includes an obligation to notify of data breaches in certain cases;
- includes an obligation to appoint a data protection officer in public agencies, big data operations and when the processing of sensitive data is a principal activity; and
- mandates the obligation to carry out an impact analysis when the data processor intends to treat personal data in such a way that there is a high risk of affecting fundamental data subject rights.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

There are no specific rules on the use of cookies or equivalent technologies. The general principles contained in the DPL will apply, particularly those on informed consent from the data subject.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

See question 6 for information on electronic marketing.

Marketing by telephone is covered by the Do Not Call Law No. 26,951. This law created a Do Not Call Registry, which allows for any individual or legal entity owner or authorised user of phone services of any kind to apply for registration to prevent contact from companies advertising, offering, selling, giving or promising goods or services.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Cloud computing services are not specifically regulated under Argentine law, but there are regulations that may have effect on the use of cloud services. The DPL applies to cloud services insofar as it entails the processing of personal data. In particular, the DPL's provisions on cross-border data transfers (see question 34), data processing (see question 32) and data security (see question 20) will be relevant.

Diego Fernández **DFER@marval.com**

Av Leandro N Alem 882
Buenos Aires
Argentina

Tel: +54 11 4310 0100
Fax: +54 11 4310 0200
www.marval.com

Australia

Alex Hutchens, Jeremy Perier and Meena Muthuraman

McCullough Robertson

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The Privacy Act 1988 (Cth) (Privacy Act), which was enacted to give effect to Australia's agreement to implement the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), governs how personal information is handled in Australia by the Commonwealth Government and private sector entities with an annual turnover of at least A$3 million (APP entities). Some small businesses (with a global aggregate group turnover of A$3 million or less) are also covered by the Privacy Act, including private health services providers that hold health information, businesses that sell or purchase personal information, credit-reporting bodies and contracted service providers for a Commonwealth contract.

'Personal information' is the conceptual equivalent in PII in other jurisdictions, and is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.

It is still unclear whether metadata, cookies and IP addresses fall within the definition of personal information. However, while it will ultimately depend on the circumstances, the better view is that they are likely to be personal information.

The Privacy Act contains 13 Australian Privacy Principles (APPs), which set out the minimum standards for dealing with personal information and are the foundation of Australian privacy law. They cover the life cycle of the collection, use, storage, disclosure and destruction of personal information. The Privacy Act also includes credit-reporting obligations that govern the way in which personal credit information about individuals must be handled by credit-reporting bodies, credit providers and other third parties.

Further, each Australian state and territory has legislation broadly equivalent to the Privacy Act that regulates the handling of personal information by public sector agencies at the state and territory level.

Australia also has specific legislation that regulates data protection in the health sector, telecommunications sector and consumer credit reporting (as outlined in question 7), and other legislation at the Commonwealth and state level that is relevant to privacy and the use of personal information, including the Spam Act 2003 (Cth) (Spam Act), which regulates electronic marketing, the Do Not Call Register Act 2006 (Cth) (Do Not Call Register Act), which regulates unsolicited commercial calls to listed phone numbers, criminal laws prohibiting unauthorised access to computer systems and various surveillance and listening-devices legislation.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Office of the Australian Information Commissioner (Information Commissioner) is responsible for overseeing compliance with the Privacy Act.

The Information Commissioner has a legislative mandate to conduct education programmes, and can also:

- conduct investigations in relation to a suspected or actual breach of the Privacy Act (whether in response to a complaint, or as an 'own motion' investigation that is made of its own volition), including by requiring a person to give information or documents, or to attend a compulsory conference and entering premises to inspect documents;
- accept enforceable undertakings from an APP entity, the breach of which can lead to a civil penalty;
- make determinations;
- seek an injunction regarding any conduct that would contravene the Privacy Act; and
- seek a civil penalty order from the Federal Court for the imposition of a statutory penalty of up to A$2.1 million for serious or repeated interference with the privacy of an individual.

Additionally, the Australian Communications and Media Authority (ACMA) regulates telecommunications, spam and telemarketing, including industry-specific privacy-related rules discussed below. The ACMA is in charge of enforcing the Spam Act and the Do Not Call Register Act and may:

- issue a formal warning;
- require an entity to give a court-enforceable undertaking, the breach of which can lead to a civil penalty;
- issue infringement notices (which are similar to on-the-spot fines) if it considers there has been a breach of the Spam Act (infringement notices can be up to A$180,000, depending on the basis for issuing the notice);
- seek an injunction regarding conduct that would contravene the Spam Act; and
- seek a civil penalty order from the Federal Court for the imposition of a statutory penalty of up to A$2.1 million for repeated breaches of the Spam Act.

The Australian Attorney-General's Department is responsible for administering lawful assistance to law enforcement agencies under the Telecommunications (Interception and Access) Act 1979, which involves regulating and enforcing privacy-related legislative schemes. Regulators under the various state-based laws for the public sector have similar powers, but these are not relevant for private sector entities in Australia.

3 Legal obligations of data protection authority

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

The Information Commissioner is not subject to any strict legal obligations to cooperate with other data protection authorities in other countries. However, the Information Commissioner also participates in several forums and arrangements to promote best privacy practice internationally, address emerging privacy issues and cooperate on cross-border privacy regulation. For example, the Information Commissioner actively participates in the Asia Pacific Privacy Authorities (APPA) Forum to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints in the Asia Pacific region.

The Information Commissioner is also co-administrator of the Cross-border Privacy Enforcement Arrangement (CPEA), which creates a framework for data protection authorities to collaborate and share information in relation to privacy investigation and enforcement across member economies and data protection authorities outside the Asia-Pacific Economic Cooperation area. Similarly, the Global Cross Border Enforcement Cooperation Arrangement (GCBECA) encourages enforcement authorities to share information about potential or ongoing privacy investigations and coordinate enforcement activities.

4 Breaches of data protection

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

Breaches of the Privacy Act can lead to administrative determinations of breach (which may or may not be accompanied by a compensation order), the acceptance of court-enforceable undertakings and, for serious or repeated interferences with privacy, a statutory penalty of up to A$2.1million for corporations.

Criminal sanctions may also be imposed where an individual or corporation fails to comply with a request or direction given by the Information Commissioner in relation to any investigation run by the Information Commissioner, or any determination regarding a breach of data protection law.

Australia's Federal Parliament introduced new mandatory data breach notification obligations in early 2017 (which took effect in February 2018) for all government agencies and businesses that are subject to the Privacy Act. Under this new regime, if a relevant agency or business suspects there has been a data breach that is likely to result in serious harm to any of the affected individuals (an 'eligible data breach'), subject to some limited exceptions, it must:

- carry out a 'reasonable and expeditious' assessment within 30 days of becoming aware as to whether there has been an eligible data breach; and
- if an eligible data breach has occurred, notify the Information Commissioner and affected individuals as soon as practicable.

Scope

5 Exempt sectors and institutions

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

The Privacy Act and the APPs apply to all APP entities, which broadly speaking include all Commonwealth Government entities and private sector entities with an annual turnover of A$3 million or more. However, some specific types of businesses or areas of activities are specifically excluded from the application of the Privacy Act, such as public hospitals and healthcare facilities, most public universities and public schools, some media organisations acting in the course of journalism, registered political parties and most small businesses (with an annual turnover of less than A$3 million).

Additionally, employee records relating to current and former employment relationships are expressly excluded from the application of the Privacy Act and the APPs.

It is worth noting that in specific circumstances some small businesses may still be captured by the Privacy Act, including where they are a private sector health provider, a service provider for the Commonwealth Government, a related entity to a business that is covered by the Privacy Act, or if they handle credit-reporting information or sell or purchase personal information.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Privacy Act governs how personal information is collected, stored and used, regardless of the medium or material that contains or communicates that information. Generally speaking, the Privacy Act and the APPs will apply to any interception, marketing or surveillance activities that involve dealing with personal information.

Additionally:

- the interception of communications is governed by the Telecommunications (Interception and Access) Act 1979 (Cth). Under this Act, a person must not intercept any communication passing through the telecommunications network without the knowledge of the persons issuing or receiving the communication;
- the use of monitoring and surveillance devices is governed by various legislation at a federal level as well as at the state and territory level. Generally speaking, the surveillance legislation prohibits the tracking and audio or video recording of any person or activity without the consent of that person or of the person involved in the activity;
- specific workplace surveillance laws exist in New South Wales, the Australian Capital Territory and, to some extent, in Victoria;
- commercial electronic messages that are sent to an email address or a phone number accessed in Australia are regulated by the Spam Act; and
- the practices of telemarketers and fax marketers must comply with the Do No Call Register Act 2006 (Cth).

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

In Australia, further laws and regulations also apply in relation to specific data protection rules and related areas as follows.

Consumer credit reporting is regulated by the Privacy Regulation 2013 and the Privacy (Credit Reporting) Code 2014, in addition to Part IIIA of the Privacy Act.

There are also specific data protection rules for the health sector in Australia, including:

- the My Health Records Act 2012 (Cth), My Health Records Rule 2016 (Cth) and My Health Records Regulation 2012 (Cth), which create the legislative framework for the Australian government's My Health Record System; and
- the Healthcare Identifiers Act 2010 (Cth), which regulates the use and disclosure of healthcare identifiers.

The telecommunications sector is subject to specific data protection rules, including the Telecommunications Act 1997 (Cth), which imposes restrictions on the use and disclosure of telecommunications and communications-related data, and the Telecommunications (Interception and Access) Act 1979 (Cth), which, among other things, regulates the interception of and access to the content of communications transiting over telecommunications networks, and stored communications (eg, SMS and emails) on carrier networks with enforcement agencies.

The following laws apply in NSW and the Australian Capital Territory in relation to workplace monitoring and surveillance: the Workplace Privacy Act 2011 (ACT), Listening Devices Act 1992 (ACT), Workplace Surveillance Act 2005 (NSW) and Surveillance Devices Act 2007 (NSW). In both jurisdictions, this legislation imposes strict requirements on employers to obtain employee permission before performing covert surveillance in the workplace.

Further, general laws on monitoring and surveillance would apply to workplace surveillance and monitoring where relevant. For instance, in addition to the Telecommunications (Interception and Access) Act 1979 (Cth), the Surveillance Devices Act 2004 (Cth) applies to the use

of surveillance devices by Australian government agencies, and the following laws at the state and territory level apply variously to the monitoring and surveillance of certain devices such as computers, cameras and electronic tracking devices:

- Surveillance Devices Act 2016 (SA);
- Listening Devices Act 1991 (Tas);
- Surveillance Devices Act 1999 (Vic);
- Surveillance Devices Act 1998 (WA); and
- Surveillances Devices Act 2007 (NT).

While the Privacy Act does not directly cover workplace surveillance, we note that private sector employers that are subject to the Privacy Act are exempted from complying with the Privacy Act in relation to employee records directly related to the employment relationship between employer and employee. Therefore, to the extent that workplace monitoring and surveillance involves the collection of personal information that is not an employee record – for example, a CCTV video recording or a digital copy of emails that do not relate to the employment of an employee – then the APPs may apply to that personal information.

8 PII formats

What forms of PII are covered by the law?

The Privacy Act covers all personal information, whether it is true or not, and whether it is recorded in a material form or not.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The reach of the law is not limited to companies based, or operating, in Australia.

The Privacy Act and the APPs will apply to any APP entity that is established in Australia, carries on business in Australia or collects personal information in Australia. This is quite broad and will capture, for example, any APP entity based outside of Australia that collects personal information about an individual located in Australia through a website hosted outside of Australia.

The Spam Act may also potentially apply in relation to any commercial electronic communication sent to an email address or a phone number accessed in Australia.

10 Covered uses of PII

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

While the Privacy Act does not refer to 'processing' personal information, it governs the collection, holding, use, disclosure, access to and correction of personal information (which in effect are all treated as a form of processing).

Unlike in other jurisdictions, where there is a clear distinction between data controllers and data processors, the Australian regime does not distinguish between those who control or own personal information and those who process personal information. Instead, the Privacy Act applies to any APP entity that collects, uses or holds personal information (ie, any APP entity that has possession or control of any record or other material that contains personal information).

In practice, this leads to parties who would usually consider themselves to be data processors to have additional obligations under the Privacy Act beyond those that they would not normally expect to have.

Legitimate processing of PII

11 Legitimate processing – grounds

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

There is no such requirement under Australian law. However, the APPs provide that an APP entity may only hold, use or disclose personal information for the primary purpose for which it was collected, or any other purpose that is related to the purpose for which the information was collected. Typically, parties in Australia have a privacy policy that explains the various uses that may be made of personal information so that it can be used for multiple purposes.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The Privacy Act distinguishes between personal information generally and sensitive information specifically. Sensitive information includes:

- any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record;
- health or genetic information about an individual; and
- biometric information and templates.

The APPs contain higher standards for the collection and use of sensitive information. Sensitive information:

- may only be collected with the express consent of the relevant individual, except in specified circumstances;
- must not be used or disclosed for any purpose other than the purpose for which it was collected, and any other purpose that is directly related to that purpose (provided the secondary purpose would be within the reasonable expectations of the relevant individual); and
- cannot be shared between members of the same corporate group in the same way that they may share other personal information.

Health information is also subject to additional requirements and restrictions under state, territory and Commonwealth legislation, as outlined above.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Yes. APP 5 requires APP entities to take such steps as are reasonable in the circumstances to notify the individual of various matters at or before the time their personal information is collected (or, if that is not practicable, as soon as practicable after collection). These matters include:

- the identity and contact details of the APP entity;
- where relevant, the fact that the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order;
- the purposes for which the information is collected;
- any other person to which the APP entity may disclose the personal information;
- that the entity's APP privacy policy contains information about how the individual may access and correct their personal information, or complain about a breach of the APPs (and how the entity will deal with such a complaint); and
- whether the entity is likely to disclose the personal information to overseas recipients, and if so, the countries in which such recipients are likely to be located.

APP entities usually comply with this requirement by having a privacy policy on their website and providing individuals with a privacy collection statement that notifies the individual of the purpose of collection and other mandatory disclosures, and refers the individual to the APP entity's privacy policy for more complete details.

14 Exemption from notification

When is notice not required?

The notification requirement in APP 5 is not an absolute requirement. It requires APP entities to take such steps as are reasonable in the circumstances to notify the individual (see question 13). This means that an APP entity does not have to notify the individual if it would be

unreasonable or impracticable to do so. The Information Commissioner has indicated that the circumstances in which it would be reasonable for an APP entity not to notify an individual include where notification is impracticable (including where the time and cost outweighs the privacy benefits), notification would jeopardise the purpose of collection, notification may pose a serious threat to the health and safety of a person or public health and safety, or where the APP entity collects information from the individual on a recurring basis.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Not specifically. As discussed in question 11, personal information must only be used for the purpose for which it was collected or reasonably related purposes; however, this does not extend to giving individuals choice or control over its use. However, individuals must be given access to their information on request, and must be able to direct that information be updated where it is no longer accurate (subject to some exceptions).

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Yes. An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects, holds, uses or discloses is accurate, up to date, complete and, having regard to the purpose of the use or disclosure, relevant. The reasonable steps that an APP entity should take will depend on the sensitivity of the information, the nature of the APP entity (ie, its size, resources and business model), the possible adverse consequences for the relevant individual if the quality of the information is not ensured and the practicability and cost of taking such steps.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

There is no specific limit on the amount of information that may be collected, or the period for which it may be held, but there are general principles that impose limits on similar grounds.

Personal information must only be collected to the extent it is reasonably necessary for the purposes of the APP entity's activities. Also, APP entities must take reasonable steps to destroy or permanently de-identify personal information if that information is no longer needed for any purpose for which it was collected or for a related purpose (unless it is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information).

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes. An APP entity can only use or disclose personal information for the purpose for which it was collected or for a related purpose (or directly related purpose in the case of sensitive information). These purposes are usually determined by reference to the purposes disclosed in the APP entity's privacy policy.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

As discussed above, generally speaking personal information may only be used for the purposes disclosed in the APP entity's privacy policy or any related purposes. There are also general exceptions that allow for further uses, including where an individual has given their consent, where the use or disclosure is required or authorised by Australian law or by a court (including tribunals and enforcement bodies), where the information is used to prevent a serious threat to the life or health of a person or for research or statistical analysis that is relevant to public health or public safety, or where personal information (other than sensitive information) is disclosed to a related entity within the same corporate group.

These exceptions do not apply to the use or disclosure by an APP entity of personal information for the purpose of direct marketing or of government-related identifiers (such as tax file numbers or social security numbers).

Security

20 Security obligations

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

An APP entity must take such steps as are reasonable in the circumstances to protect the personal information it holds or control from misuse, interference and loss, as well as unauthorised access, modification or disclosure. This is not an absolute standard, and varies in the circumstances, which include the nature of the APP entity, the amount and sensitivity of the personal information, the possible adverse consequences for an individual in case of a breach, the practicability and cost of implementing security measures and whether a security measure is in itself privacy-invasive.

There are additional information security requirements for credit-reporting bodies, credit providers and some tax and healthcare services providers.

21 Notification of data breach

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?

As discussed above, Australia's Federal Parliament introduced new mandatory data breach notification obligations in early 2017 (which took effect in February 2018) for all government agencies and businesses that are subject to the Privacy Act. Under this new regime, if a relevant agency or business suspects there has been a data breach that is likely to result in serious harm to any of the affected individuals ('eligible data breach'), subject to some limited exceptions, it must:

- carry out a reasonable and expeditious assessment within 30 days of becoming aware as to whether there has been an eligible data breach; and
- if an eligible data breach has occurred, notify the Information Commissioner and affected individuals as soon as practicable.

These provisions replace the existing voluntary data breach notification guidelines that were released by the Information Commissioner, which recommend that, if there is a 'real risk of serious harm' as a result of a data breach, the affected individuals and the Information Commissioner should be notified.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The Privacy Act does not require an APP entity to appoint a data protection officer, although it is generally accepted best practice to have at least a person or department responsible for data security and privacy-related matters. This person or department would be the first point of contact for any queries or complaints from the public or the Information Commissioner.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

While the Privacy Act does not outline specific internal process or documentation requirements, there are some obligations under the Privacy Act that are demonstrably easier to prove with appropriate records.

Notably, APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs. The Information Commissioner has released a Privacy Management Framework that outlines four steps it expects APP entities to take to meet its ongoing compliance obligations under APP 1. Specifically, an APP entity should ensure it:

- has a culture of privacy and values personal information;
- develops and implements effective privacy practices, procedures and systems;
- examines and reviews the effectiveness and appropriateness of its privacy practices, procedures and systems; and
- tries to anticipate future privacy issues.

In particular, in relation to the second and third points, documentation that demonstrates an analysis of the APPs and the measures taken to comply with them will be a valuable artefact if the Information Commissioner ever conducts an investigation.

Finally, APP 1 requires that all APP entities implement and maintain a privacy policy that must cover various mandatory matters and also describe the company's information-handling practices generally.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The Privacy Act does not expressly require a privacy-by-design approach to new data processing operations. However, as set out above, APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems to ensure compliance with their privacy obligations. This requirement is qualified by a 'reasonable steps' test, which is intended to provide entities with the flexibility to implement practices, procedures and systems based on its circumstances, including the type of personal information collected and the potential adverse consequences if such information were not handled in compliance with the Privacy Act, but it is recognised that best practice compliance with this principle will involve consideration of privacy-by-design norms.

Additionally, while not expressly required under the Privacy Act, the Information Commissioner strongly encourages entities to carry out privacy impact assessments as part of their risk management process and to ensure compliance with the Privacy Act, and has published a guide to undertaking such privacy impact assessments.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

No registration is required. However, small businesses or not-for-profit organisations not usually covered by the Privacy Act may choose to be treated as an organisation for the purposes of the Privacy Act and therefore be subject to the APPs, in which case they will need to apply to the Information Commissioner to be placed on the public Opt-in Register.

26 Formalities

What are the formalities for registration?

No registration fee is payable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

The Opt-in Register is publicly available on the Information Commissioner's website.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Entry on the Opt-in Register is a public declaration that an entity agrees to become an APP entity and to be treated as an organisation under the Privacy Act.

31 Other transparency duties

Are there any other public transparency duties?

As set out above, APP 1 provides that APP entities must manage personal information in an open and transparent way. Relevantly, APP 1 requires APP entities to have a clearly expressed and up-to-date privacy policy available free of charge and in an appropriate form about how it manages personal information, including:

- the kinds of personal information collected and held by the entity;
- how personal information is collected and held;
- the purposes for which personal information is collected, held, used and disclosed;
- how an individual may access their personal information and seek its correction;
- how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled; and
- whether the entity is likely to disclose personal information to overseas recipients, and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

The Information Commissioner's APP Guidelines provide further guidance on the types of information that should be included in a privacy policy.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Because the Privacy Act does not make the distinction between a data 'controller' and 'processor', all transfers and disclosures of personal information to a third party are treated the same way (other than companies within the same group of companies), regardless of the purpose of the transfer or disclosure, and an APP entity must comply with the APPs in relation to all transfers or disclosures of personal information.

However, where an APP entity discloses personal information to entities that provide outsourced processing services, it remains liable for any act or practice of the service provider that would breach the APPs.

See the restrictions in relation to cross-border transfer in question 34.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

There are no restrictions on the disclosure of personal information (other than disclosure requirements and purpose limitations, as discussed above).

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

There is no prohibition against 'disclosing' personal information outside Australia (disclosure is broader than 'transfer' and may include allowing an overseas-based person to access information that is physically stored in Australia), but, under APP 8, an APP entity is required to take reasonable steps to ensure that an overseas recipient will handle

an individual's personal information in accordance with the APPs, and the APP entity will be deemed liable for the acts of the overseas entity if those acts would amount to a breach of the APPs in Australia if done by the disclosing entity in Australia.

There is an exception to the 'deemed liability' provisions if the relevant individual consents to the disclosure of their personal information outside of Australia and is told that by consenting their information will not be treated in accordance with the APPs. This exception is relatively new and is not widely relied on.

Some categories of personal information are subject to additional rules. In particular, if sensitive information is disclosed overseas, more rigorous steps may be required to ensure the recipient does not breach the APPs, and there are some restrictions on sending information held in the Australian credit-reporting system overseas. Further, the legislation governing Australia's My Health Record system prohibits My Health Record operators and service providers from holding, taking, processing or handling relevant health records outside of Australia (or enabling others to do so). The transfer of health information between states is also limited by some state and territory health privacy acts.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

An entity does not need to notify or obtain authorisation from any supervisory authority for the cross-border transfer of personal information. However, it must include in its privacy policy a list of all countries to which it is likely to disclose personal information.

36 Further transfer

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.

Rights of individuals

37 Access

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

Individuals have the right under APP 12 to request access to their personal information held by APP entities. A reasonable fee may be charged for access, and the APP entity must comply with the request. However, there are circumstances in which such a request can be refused, including where it would pose a serious threat to the life, health or safety of any individual or to public health or safety, where it would have an unreasonable impact on the privacy of other individuals, where granting access would disclose commercially sensitive information, where the request is frivolous or vexatious, or in circumstances relating to legal proceedings and enforcement activities.

Information held by Commonwealth government agencies is subject to public freedom of information laws, but these do not apply to private sector entities.

38 Other rights

Do individuals have other substantive rights?

An individual may request an APP entity to correct the personal information about that individual, in which case the entity must take reasonable steps to correct the information to ensure that, having regard to the purpose for which the information is held, it is accurate, up to date, complete, relevant and not misleading.

If the individual's request is not granted, the individual can insist that the entity place a note on its files to the effect that the request has been made and has not been granted.

Further, individuals have the right to deal anonymously with an APP entity or by pseudonym, unless this is impractical for the entity, or the entity is required or authorised by law or a court or tribunal order to deal with identified individuals.

Where an APP entity is authorised to use or disclose personal information for the purpose of direct marketing, it is a condition of the authority that the relevant individual has the right and means to easily request not to receive direct marketing communications from the entity.

If an individual believes that any APP entity is not handling its personal information in accordance with the Privacy Act, it has a right to lodge a complaint with the Information Commissioner.

39 Compensation

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?

Where the Information Commissioner is satisfied that there has been a breach of the Privacy Act, the Commissioner may order a range of remedies, including a declaration that compensation must be paid for any loss or damage suffered because of the act or practice that caused the complaint.

In the case of serious or repeated interference with the privacy of an individual, the Information Commissioner may also seek civil penalty orders before the Federal Court of up to A$360,000 for individuals and up to A$2.1 million for companies. An act or practice is an 'interference with the privacy' of an individual if it breaches the APPs in relation to personal information about the individual.

Other orders include injunctions and orders to give a public apology. Compensation orders are not subject to any particular monetary limit, but are generally in the low thousands of Australian dollars.

40 Enforcement

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

Australian law currently does not allow an individual to make a claim directly against an APP entity for a breach of the Privacy Act. Any complaint about how an APP entity collects and handles personal information must go through the Information Commissioner, who may then take appropriate actions such as investigating the complaint or seeking a court order.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Not applicable.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, most decisions and orders made by the Information Commissioner can be appealed before and reviewed by the Administrative Appeal Tribunal or the Federal Court, depending on the decision or order.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

It is not clear whether cookies actually satisfy the definition of personal information in Australia. However, it is best practice (and the better view) to treat them as if they were indeed covered by the Privacy Act. Cookie-based marketing activities that involve the collection of personal information are permissible, provided the notice and consent requirements under the APPs are complied with by, for example, describing the activities in the privacy policy.

It is also best practice to comply with the Australian Guideline for Online Behavioural Advertising, which is a self-regulatory guideline for third-party online behavioural advertising. The guideline has been developed by a group of leading business and industry associations in

the online advertising sector called the Australian Digital Advertising Alliance (ADAA), and signatories include leading domestic and international digital businesses.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

As a general requirement, any use of personal information for direct marketing activity must comply with APP 7, which imposes strict rules on what information can be used, and gives individuals the right to opt out of marketing activity.

Additionally, the Spam Act 2003 prohibits the sending of unsolicited commercial electronic messages (spam) without consent. Consent can be express or inferred from business or other relationships (although the Courts in Australia have held that these need to be pre-existing relationships). All commercial electronic messages must have a functional unsubscribe facility included in the message.

Further, the Do Not Call Register Act 2006 (Cth) prohibits unsolicited telemarketing calls being made and unsolicited marketing faxes being sent to any numbers registered on the Do Not Call Register. Telemarketers, researchers and fax marketers must also comply with enforceable industry standards including the Telemarketing and Research Calls Industry Standard 2007 and the Fax Marketing Industry Standard 2011.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Cloud services are treated no differently from other services under the Privacy Act. However, by their nature, they are more likely to trigger the 'overseas disclosure' requirements described in APP 8, which means that the location of overseas disclosures has to be included in the APP entity's privacy policy, and a deemed liability regime applies so that the acts of the cloud provider are deemed to be the acts of the information owner.

Generally speaking, these issues are typically managed through pre-contractual due diligence to ensure the provider has robust data-handling practices, and the use of contractual measures that seek to flow down the requirements of the Privacy Act on to the cloud service provider, together with general obligations to take reasonable steps to ensure the security of information, restricting the purposes for which information can be used, and to require notification of any breaches.

Lawyers | McCullough Robertson

Alex Hutchens **ahutchens@mccullough.com.au**
Jeremy Perier **jperier@mccullough.com.au**
Meena Muthuraman **mmuthuraman@mccullough.com.au**

Level 32, MLC Centre,
19 Martin Place,
Sydney, NSW, 2000
Australia

Tel: +61 2 8241 5609
Fax: +61 2 8241 5699
www.mccullough.com.au

Austria

Rainer Knyrim

Knyrim Trieb Attorneys at Law

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legislative framework for the protection of personally identifiable information (PII) in Austria mainly consists of the EU General Data Protection Regulation (GDPR) and the Data Protection Act (ADPA), which implements the mandatory opening clauses and provisions of the GDPR. In addition, the ADPA enshrines the fundamental right to data protection at the constitutional level. Furthermore, privacy-related provisions can be found in the Telecommunications Act regarding electronic advertising and the processing of personal communication data of users by telecommunication service providers, in the Act on Banking regarding banking secrecy and in the Collective Labour Relations Act regarding data applications for purposes of personnel administration and evaluation. In the field of healthcare, the Health Telematics Act 2012 (along with the Health Telematics Regulation and the Federal Electronic Health Record Regulation 2013) states that technical data security measurements must be implemented for the transmission of health data among health service providers and contains provisions for the implementation and operation of the Federal Electronic Health Record. The Research Organisation Act regulates data processing for research purposes by scientific institutions.

Chapter 3 of the ADPA implements the Directive (EU) 2016/680 and regulates the processing of PII for purposes of the security police, including the protection of public security by the police, the protection of military facilities by the armed forces, the resolution and prosecution of criminal offences, the enforcement of sentences and the enforcement of precautionary measures involving the deprivation of liberty.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Data Protection Authority (DPA) shall safeguard data protection in accordance with the provisions of the GDPR and the Federal Data Protection Act. The DPA shall exercise its powers also in relation to the highest governing bodies or officers referred to in article 19 of the Federal Constitutional Law and in relation to the President of the National Council, the President of the Court of Auditors, the President of the Supreme Administrative Court and the Chairman of the Ombudsman Board in the area of the administrative matters to which they are entitled.

The DPA is established as a national supervisory authority pursuant to article 51 GDPR. The DPA acts as an authority supervising staff and as a human resource department. During his or her term of office, the head must not exercise any function that:

- could cast doubt on the independent exercise of his or her office or impartiality;
- prevents him or her from performing their professional duties; or
- puts essential official interests at risk.

The head is required to report functions that he or she exercises alongside his or her office as the head of the DPA to the Federal Chancellor without delay. The Federal Chancellor can request information from the head of the DPA on matters to be dealt with by the Authority. The head of the DPA has to meet this request only insofar as it does not impair the complete independence of the supervisory authority as described in article 52 of the GDPR.

Every data subject has the right to lodge a complaint with the DPA if he or she considers that the processing of his or her PII infringes the GDPR or section 1 of the ADPA.

The DPA shall be responsible for imposing fines on natural and legal persons within the limits of its powers. Pursuant to section 11 ADPA the DPA will apply the catalogue of article 83, paragraphs 2 to 6 GDPR in such a way that proportionality is maintained. In accordance with article 58 GDPR, the DPA will make use of its remedial powers, in particular by issuing warnings, especially in the event of initial infringements.

The ADPA empowers the DPA with further powers in addition to the investigative powers under article 58 GDPR. The DPA can request from the controller or the processor of the examined processing all necessary clarifications and inspect data processing activities and relevant documents. The controller or processor shall render the necessary assistance. Supervisory activities are to be exercised in a way that least interferes with the rights of the controller or processor and third parties.

For the purposes of the inspection, the DPA shall have the right, after having informed the owner of the premises and the controller or processor, to enter rooms where data processing operations are carried out, put data processing equipment into operation, carry out the processing operations to be examined and make copies of the storage media to the extent strictly necessary to exercise its supervisory powers.

In case a data processing operation causes serious immediate danger to the interests of confidentiality of the data subject that deserve protection (imminent danger), the DPA may prohibit the continuation of the data processing operation by an administrative decision pursuant to section 57, paragraph 1 of the General Administrative Procedure Act 1991. The continuation may also be prohibited only partially if this seems technically possible, meaningful with regard to the purpose of the data processing operation and sufficient to eliminate the danger. At the request of a data subject, the DPA can also order, by an administrative decision pursuant to section 57, paragraph 1 of the General Administrative Procedure Act, the restriction of processing pursuant to article 18 GDPR if the controller does not comply with an obligation to that effect within the period specified. If prohibition is not complied with immediately, the DPA shall proceed pursuant to article 83, paragraph 5 GDPR.

3 Legal obligations of data protection authority

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

The rules governing cooperation between the lead supervisory authority and the other supervisory authorities concerned are laid down in

article 60 GDPR. Article 61 GDPR provides for provisions on mutual assistance between the supervisory authorities. Pursuant to article 62 GDPR, the supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other member states are involved. In order to contribute to the consistent application of the GDPR, article 63 GDPR establishes a consistency mechanism according to which the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in section 2 of the GDPR.

4 Breaches of data protection

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

Beside the penalty provisions under the GDPR, breaches of data protection regulations can lead to criminal or administrative penalties. The third section of the ADPA provides specifying regulations regarding the implementation of remedies, liability and penalties. The implementation of administrative fines provides, to a certain extent, a possibility to impose fines primarily on legal persons.

The DPA shall be able to impose a fine on a legal person if one of its company organs or managers as decision maker or with a controlling position is subject to negligence or a breach of supervision. According to the concept of the Austrian administrative penal provisions, such fines would be imposed on the managing or executive board unless a responsible representative is appointed. The DPA shall refrain from imposing a fine on a responsible party pursuant to section 9 of the Administrative Penal Act 1991, if an administrative fine has already been imposed on the legal person for the same infringement.

No fines may be imposed on public authorities, public entities or public bodies, such as bodies established in particular under public or private law, which act on a statutory basis.

Whoever, with the intention of unlawfully enriching himself or a third party, or with the intention of damaging another person's claim guaranteed according to section 1, paragraph 1 ADPA, deliberately uses PII that has been entrusted to or has become accessible to him or her solely because of this professional occupation, or that he or she has acquired illegally, for him or herself or makes such data available to another person or publishes such data despite the data subject's interest in confidentiality, shall be punished by a court with imprisonment of up to one year unless the offence is subject to a more severe punishment pursuant to another provision.

Other provisions may be found in the Austrian Criminal Law, which contains rules for punishments in case of violations concerning data (eg, intentionally altering or deleting data).

Unless the offence meets the elements of article 83 GDPR or is subject to a more severe punishment according to other administrative penal provisions, an administrative offence punishable by a fine of up to €50,000 is committed by anyone who:

- intentionally and illegally gains access to data processing or maintains an obviously illegal access;
- intentionally transmits PII in violation of the rules on confidentiality and, in particular, intentionally uses data entrusted to him or her pursuant to the provisions granting the use of PII for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or of address data to inform or interview data subjects for other purposes;
- intentionally acquires PII in case of emergency under false pretences violating section 10 ADPA;
- processes images contrary to the provisions of Chapter 1, Part 3 ADPA; or
- refuses inspection pursuant to section 22, paragraph 2 ADPA.

Attempts shall be punishable. The penalty for the forfeiture of data storage media and programs as well as image transmission and recording devices may be imposed if these items are connected with an administrative offence.

The DPA shall be responsible for imposing fines on natural and legal persons within the limits of its powers. Pursuant to section 11 ADPA, the DPA will apply the catalogue of article 83, paragraphs 2 to 6 GDPR in such a way that proportionality is maintained. In accordance with article 58 GDPR, the DPA will make use of its remedial powers, in particular by issuing warnings, especially in the event of initial infringements.

Scope

5 Exempt sectors and institutions

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

As a consequence of the constitutional status of the right for the protection of PII, the data protection law is applicable in all sectors. No type of organisation is exempted. Both public authorities and private organisations have to obey the rules imposed by data protection law. Pursuant to section 30, paragraph 5 ADPA, no fines may be imposed on authorities, public law corporate bodies or public entities, in particular entities established under public or private law, that act on a statutory basis.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Since each of these activities regularly leads to the electronic use of PII, the provisions of the GDPR and ADPA are generally applicable in these matters. Areas such as telecommunication or electronic marketing are regulated in the Telecommunications Act and the E-Commerce Act. The Criminal Law includes specific rules for punishments, for example, in the case of intentionally breaching the secrecy of telecommunication or abusively intercepting transferred data. The right to contradict the transmission of personally addressed advertisement material is defined in section 151, paragraph 11 of the Trade Regulation Act. Monitoring employees and appraising their performance is governed by the Collective Labour Relations Act, which, to the extent of the respective provisions, also forms part of Austrian data protection law. The ADPA regulates the permissibility of recording images and provides for special data security and labelling measures.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

A specific act exists for the transmission of health data among health service providers and for the Austrian Electronic Health Record, but with respect to the core regulations of data protection, this act refers to the GDPR. The same is true for regulations on credit information: credit information databases are mentioned in a few acts referring to data protection, which have incorporated general provisions to be applied to various areas connected to the processing of PII. The E Government Act provides regulations for a Federal Identity Management to enable authorities to identify people uniquely in governmental proceedings. The Act also regards aspects of data protection by defining an identity management system that prevents the possibility of merging PII across multiple authorities. If smart meters are used for the supply of electricity or gas, the applicable acts contain provisions for the protection of PII and grant customers the right to have their data accessed or transmitted via the internet (Electricity Industry and Organisation Act 2010, Gas Industry Act 2011). The Research Organisation Act establishes specific data protection regulations for scientific or historical research purposes or statistical purposes. Pursuant to the Collective Labour Relations Act, the implementation of control measures and technical systems for the control of employees, provided that these measures affect human dignity, require the consent of works councils in order to be legally valid.

8 PII formats

What forms of PII are covered by the law?

In general, all activities regarding (partly) automatically processed PII are covered by the ADPA.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The GDPR applies to the processing of PII in the context of activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of PII of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.

The ADPA applies to the use of PII in Austria, and outside Austria insofar as the data is used in other member states of the EU for the purposes of the main establishment or a branch establishment of the data controller in Austria. Apart from this general rule, however, the law of the state in which the data controller has its seat applies where a data controller in the private sector whose seat is in another EU member state uses PII in Austria for purposes that cannot be attributed to any of the data controller's establishments in Austria. Furthermore, the ADPA shall not be applied insofar as the data is only transmitted through Austrian territory. A revision of the territorial scope in the course of the amendment to the ADPA failed owing to the lack of a constitutional majority in the Austrian parliament.

10 Covered uses of PII

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

The GDPR gives broad cover to the processing of PII; any type of processing such as collecting, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction is covered by its provisions.

The controller shall be responsible for, and be able to demonstrate the compliance with, the provisions and principles of the GDPR relating to the processing of PII. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject (article 28, paragraph 1 GDPR). Processing by a processor shall be governed by a contract or other legal act under EU or member state law that is binding on the processor with regard to the controller and sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of PII and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate the requirements laid down in article 28, paragraph 3 GDPR. Both the controller and the processor shall designate a data protection officer under certain conditions, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk and must keep a record of processing activities, whereas the content of the record of the processor must meet less stringent requirements.

Legitimate processing of PII

11 Legitimate processing – grounds

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

Statutory provisions regarding the data subject's consent and legitimate purpose for processing and transmission of PII have been harmonised with the GDPR as set in Chapter 2 'Principles' of the GDPR.

In the case of an offer of information society services directly to a child, consent to the processing of PII of a child pursuant to article 6, paragraph 1(a) GDPR shall be lawful where the child is at least 14 years old (section 4, paragraph 4 ADPA).

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Pursuant to article 9, paragraph 1 GDPR, processing of special categories of PII (information 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 be prohibited, unless a condition laid down in article 9, paragraph 2 GDPR is met.

The Health Telematics Act 2012 provides for special legal provisions for the electronic transfer of personal health data and genetic data.

Further, the ADPA contains reworded provisions for special data processing activities that are adapted to meet the preconditions of the GDPR. The Austrian legislator reworded new provisions on 'image processing' that cover every observation of events. This leads to an extended scope (eg, photographs shall also be covered).

Processing PII on acts or omissions punishable by courts or administrative authorities, in particular concerning suspected criminal offences, as well as data on criminal convictions and precautionary measures involving the deprivation of liberty, is permitted if the requirements of the GDPR are met and if:

- an explicit legal authorisation or obligation to process such data exists; or
- the legitimacy of the processing of such data is otherwise based on statutory duties of diligence, or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party pursuant to article 6, paragraph 1(f) of the GDPR, and the manner in which the data is processed safeguards the interests of the data subject according the GDPR and the ADPA.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Pursuant to the provisions of the GDPR, controllers are required to provide information to data subjects whose PII is processed. If PII is collected directly from the data subject, the controller must provide information laid down in article 13 GDPR. If PII has not been obtained directly from the data subject, the controller has to provide, in addition to the information listed in article 13 GDPR, the categories of PII concerned from which source the PII originates and, if applicable, whether it came from publicly accessible sources (article 14 GDPR).

14 Exemption from notification

When is notice not required?

In addition to the exceptions pursuant to article 13, paragraph 4 and article 14, paragraph 5 GDPR, the Second Data Protection Amendment Act 2018 regulates exceptions from the obligation to provide information within the framework of the laws concerning healthcare professionals.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The ADPA follows the provisions of the GDPR in this question. Section 4, paragraph 2 ADPA provides for a restriction of the right of rectification and the right to erasure. If PII processed by automated means cannot be rectified or erased immediately because it can be rectified or erased only at certain times for economic or technical reasons, processing of the PII concerned shall be restricted until that time, with the effect as stipulated in article 18, paragraph 2 of the GDPR.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The GDPR applies directly and there are no stricter rules for principles relating to processing of PII set down in the ADPA. Therefore, PII must be accurate and kept up to date. Inaccurate or outdated data shall be deleted or amended, and data controllers are required to take 'every reasonable step' to comply with the principles set forth in the GDPR.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Requirements regarding the amount and duration of data holding in the GDPR apply directly; there are no stricter rules or specifications for data storage durations set down in the ADPA. Specific storage periods can be found in the respective national material laws.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The GDPR applies directly and there are no stricter rules for principles relating to the processing of PII set down in the ADPA.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The ADPA does not require any other obligations regarding the processing of PII for purposes other than those for which the PII was initially collected than those set out in the GDPR.

Pursuant to section 7 ADPA, PII may be further used for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under one of the following conditions:

- the PII is publicly accessible;
- the PII was initially collected lawfully by the controller for other research projects or other purposes;
- the PII is pseudonymised personal data for the controller, and the controller cannot establish the identity of the data subject by legal means;
- the PII is used for these purposes to a legal provision;
- the data subject has given his or her consent; or
- the DPA has given its approval.

Even in cases where the processing of PII for scientific research purposes or statistical purposes is permitted in a form that allows the identification of data subjects, the data shall be encoded without delay so that the data subjects are no longer identifiable if specific phrases of scientific or statistical work can be performed with pseudonymised data. Unless otherwise expressly provided for by law, data in a form that allows the identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistical work to keep them identifiable.

The Research Organisation Act also specifies more detailed provisions for the processing of PII for research purposes by scientific institutions.

Security

20 Security obligations

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

The ADPA does not require any other or stricter obligations for the security of processing than those set out in the GDPR. Additionally, there are further provision for image processing (CCTV) regarding specific data security measures and labelling. Beside the duty of the controller using image processing to put up appropriate signs, they have to ensure that the access and manipulation of records by unauthorised persons are excluded. Any use of image processing has to be documented; this does not apply to real-time observation. Some of the material laws provide for specific data protection security obligations (eg, Research Organisation Act, Health Telematics Act 2012).

21 Notification of data breach

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?

Regarding this question, the GDPR applies directly.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The designation of a data protection officer (DPO) is mandatory under the conditions of article 37 GDPR.

The obligations of the DPO are laid down in section 5 ADPA. Without prejudice to other obligations of confidentiality, DPOs and persons working for the DPO shall be bound by confidentiality when fulfilling their duties. This shall apply in particular in relation to the identity of data subjects who applied to the DPO, and to circumstances that allow identification of these persons, unless the data subject has expressly granted a release from confidentiality. The DPO and persons working for the DPO may exclusively use information made available to fulfil their duties and shall be bound by confidentiality even after the end of their activities.

Section 5 ADPA provides for rules on the right of the DPO and persons working for the DPO to refuse to give evidence. Within the scope of the DPO's right to refuse to give evidence, his or her files and other documents are subject to a ban on seizure and confiscation.

Public-sector DPOs are not bound by any instructions when exercising their duties. The highest governing bodies or officers have the right to obtain information on matters to be dealt with from a public-sector DPO. The DPO shall only comply with this to the extent that this does not contradict the independence of the DPO within the meaning of article 38, paragraph 3 GDPR. Public-sector DPOs shall regularly exchange information, in particular with regard to ensuring uniform data protection standards.

Considering the type and scope of data processing activities and depending on the facilities of a federal ministry, one or several DPOs shall be appointed in the sphere of responsibilities of each federal ministry. These DPOs shall be employed by the relevant federal ministry or the relevant subordinate office or other entity.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The GDPR applies directly. In order to demonstrate compliance with the GDPR, the controller or processor should maintain records of processing activities under their responsibility. Each controller and processor shall be obliged to cooperate with the supervisory authority and make those records available to the authority upon request.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The ADPA does not alter the provisions of the GDPR, but Austrian legislation has made use of the opening clause of article 35, paragraph 10 GDPR with regard to certain legal provisions of national material laws and has carried out a data protection impact assessment as part of a general impact assessment in the context of the adoption of that legal provision (eg, Research Organisation Act).

Update and trends

The time since 25 May 2018 has seen many requests from data subjects for data access and data deletion, which showed various open questions regarding data subjects' rights in the GDPR. Currently, companies are looking forward to the first case law under the GDPR and the ADPA by the Austrian Data Protection Authority and courts relating to data subjects' rights and regarding fines.

A decision of the Austrian Constitutional Court confirmed at the end of 2017 that an Austrian supervisory authority (in this case, the Austrian Financial Market Authority) is in the position to impose fines on companies even if those fines amount to several millions of euros. Therefore, a hot topic will be if this case law will be applicable to the Austrian Data Protection Authority as well.

The next hot topic will be the ePrivacy Regulation and its relationship with the GDPR.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

According to current law, there is no legal obligation to notify or register data processing activities with the supervisory authority. The former Austrian Data Processing Register held by the DPA shall be maintained by the DPA until 31 December 2019 for archiving purposes. No entries or changes in content have been made in the Data Processing Register since 25 May 2018. Registrations in the Data Processing Register become invalid. Any person may inspect the Register. Inspection of the registration file including any authorisations contained therein shall be granted if the person applying for inspection can satisfactorily demonstrate that he or she is a data subject, and as far as no overriding interests in confidentiality on the part of the controller or another person are an obstacle to access.

26 Formalities

What are the formalities for registration?

There is no duty to file a notification with the Data Processing Register because the obligation to notify is no longer applicable. The Data Processing Register is accessible online as an archive until December 2019.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

The provision regarding penalties is no longer applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The administrative procedure to register data applications was eliminated on 25 May 2018.

29 Public access

Is the register publicly available? How can it be accessed?

Until December 2019, access to the Online Data Processing Register and its database is available at https://dvr.dsb.gv.at; from then on the internet platform will be discontinued.

30 Effect of registration

Does an entry on the register have any specific legal effect?

For changes under the Data Protection Amendment Act 2018, see question 25.

31 Other transparency duties

Are there any other public transparency duties?

The GDPR is applicable directly. With regard to the processing of images, section 13, paragraph 5 ADPA stipulates a special labelling obligation.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The ADPA contains no specific rules. Regarding the transfer of employees' data, the draft of the Data Protection Amendment Act 2018 referred in one of the opening clauses to the provisions of the Collective Labour Relations Act. However, this reference to the Collective Labour Relations Act was deleted by the Data Protection Deregulation Act 2018.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

The provisions of the GDPR apply directly. Specific restrictions concerning the disclosure of PII can be found in particular national laws (eg, Research Organisation Act).

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The provisions of the GDPR apply directly. Pursuant to the provisions of the GDPR, international data transfer outside of the EU is similar to the existing regime under the Data Protection Directive. Data can be transferred under a Commission Adequacy Decision (eg, EU–US Privacy Shield, Standard Contractual Clauses, Binding Corporate Rules or the explicit consent of the data subject). The DPA's approval for the transfer should no longer be required.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

The provisions of the GDPR apply directly. Instead of the former duty to notify with the DPA for the purpose of registration in the public Data Processing Register, the GDPR requires internal records of processing activities.

36 Further transfer

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

The GDPR applies directly and there are no stricter rules set down in the ADPA.

Rights of individuals

37 Access

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

The right to access data is part of the rights of data subjects in connection with transparency. The GDPR stipulates which information has to be provided where PII is collected from the data subject. Pursuant to section 4, paragraph 5 ADPA, the right to access pursuant to article 15 GDPR does not apply to a controller acting on a statutory basis, without prejudice to other legal restrictions, if the provision of such access jeopardises the performance of a task assigned to the controller by law. Furthermore, the right to access pursuant to article 15 GDPR does generally not apply to a controller, without prejudice to other legal restrictions, if the disclosure of such information would endanger a business or trade secret of the controller or third parties (section 4, paragraph 6 ADPA).

38 Other rights

Do individuals have other substantive rights?

Besides the right of access, data subjects have the right to request from the controller rectification or erasure of PII or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability. Furthermore, data subjects 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.

39 Compensation

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 allows data subjects to take action against data protection violations, in addition to any imposed administrative fines under the GDPR. The subject may address civil courts in order to receive compensation for any material or non-material damage suffered as a result of a GDPR infringement. Non-material damages are compensated only in exceptional cases under Austrian civil law. The ADPA also provides a choice of the competent court in whose jurisdiction the place of the domicile of the data subject and the seat of the defendant is situated.

40 Enforcement

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

Every data subject has the right to lodge a complaint with the DPA if the data subject is of the opinion that the processing of PII infringes the GDPR or the ADPA. The Federal Administrative Court shall decide through a panel of judges on complaints against administrative decisions of the DPA. Furthermore, each data subject can apply to the Federal Administrative Court if the DPA does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged.

Under the ADPA, data subjects are entitled to mandate a not-for-profit body, organisation or association that has been properly constituted, has statutory objectives that are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their PII to lodge the complaint on his or her behalf and to exercise the rights referred to in sections 24 to 27 ADPA. On the other hand, the ADPA does not provide the opportunity to assign specialised organisations (data protection NGOs) to file claims for damages with the responsible civil court.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Section 9 ADPA implements the opening clause provided by article 85 GDPR. The processing of PII by media owners, editors, copy editors and employees of a media undertaking or media service within the meaning of the Media Act, for journalistic purposes of the media undertaking or media service, the provisions of the ADPA and Chapters II, III, IV, V, VI, VII and IX of the GDPR shall not apply. When exercising its powers towards the persons named in the first sentence, the DPA must observe the protection of editorial confidentiality (section 31 Media Act).

If it is necessary to reconcile the right to protection of personal data with the freedom of expression and information, Chapters II (with the exception of article 5), III, IV (with the exception of articles 28, 29 and 32), V, VI, VII and IX do not apply to processing for purposes of academic, artistic or literary expression. Of the provisions of the ADPA, section 6 (confidentiality of data) shall be applied in such cases.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Data subjects may appeal against decisions of the DPA to the Federal Administrative Court and may further appeal against decisions of the Federal Administrative Court to the Supreme Administrative Court.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

These issues have to be evaluated under general principles and according to the provisions of the GDPR and the Telecommunications Act respectively. As the EU ePrivacy Directive 2002/58/EC has been amended by Directive 2009/136/EC, new special regulations for the declaration of consent for the use of cookies on websites had to be translated to the Telecommunications Act.

Austria implemented the EU ePrivacy Directive in November 2011 and has simply translated article 5, paragraph 3 of the Directive into section 96, paragraph 3 of the Telecommunications Act.

KNYRIM.TRIEB
RECHTSANWÄLTE

Rainer Knyrim **kt@kt.at**

Mariahilfer Straße 89A,
1060 Vienna,
Austria

Tel: +43 1 909 30 70
Fax: +43 1 909 36 39
www.kt.at

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Both the Telecommunications Act and the e-Commerce Act contain provisions for commercial communications and sanctions for 'cold-calling' and unsolicited faxes and emails. Commercial calls and the transmission of commercial messages are only legitimate with the recipient's prior consent. Some exceptions exist for the transmission of emails. Violating these provisions could lead to a fine of up to €37,000 for each unlawful email or up to €58,000 for each cold call respectively.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

The ADPA does not contain specific rules regarding the use of cloud computing services. Hence, the general provisions of the GDPR are applicable. As cloud service providers are often located outside the EEA, international data transfer needs special attention (see question 34).

According to the Health Telematics Act 2012, it has to be ensured that health data is saved in storage that is provided based on the needs of clients ('cloud computing') only if the health data has been encrypted using state-of-the-art technology (section 6, paragraph 1 No. 2 Health Telematics Act 2012).

Belgium

Aaron P Simpson, David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

As of 25 May 2018, the EU General Data Protection Regulation (GDPR) has become directly applicable in Belgium.

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) has been 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.

As a second step in adjusting the Belgian legal framework to the GDPR, a draft Bill of a new Data Protection Act (the Bill) was submitted to the Belgian Parliament on 11 June 2018. The Bill is aimed to address the areas where the GDPR leaves room for EU member states to adopt country-specific rules and to implement Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (the Directive). The Bill still needs to be adopted by the Belgian Parliament. Once the Bill is adopted, it will replace the Act on the Protection of Privacy in relation to 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 PII by police and criminal justice authorities in detail. The responses reflect the requirements set forth by the GDPR and the Bill. As the Bill has not been officially adopted by the Belgian Parliament yet, the legislative framework may still change.

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

- the 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 PII. 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.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Belgian Commission for the Protection of Privacy has been replaced by the Belgian DPA. The DPA is responsible for overseeing compliance with data protection law in Belgium. The DPA is headed by a president and consists of six main departments:

- an executive committee that, among others, approves the DPA's annual budget and determines the strategy and management plan;
- a general secretariat that supports the operations of the DPA and has a number of executive tasks, including establishing the list of processing activities that require a data protection impact assessment, rendering opinions in 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 first line 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 PII processing and recommendations regarding social, economic or technological developments that may have an impact on PII processing;
- an investigation service that is responsible for investigating data protection law infringements; and
- a litigation chamber that deals with administrative proceedings.

In addition, 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 has been 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 PII and the notification thereof to data recipients;
- order the withdrawal of a licence given to a certification body;
- impose penalty payments and administration sanctions; and
- suspend data transfers.

Furthermore, 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 PII 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.

3 Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with 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 with respect to the free flow of PII 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 EU set forth in the GDPR will apply in cross-border cases.

4 Breaches of data protection

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 set forth in the GDPR. Depending on the nature of the violation, these administrative sanctions can go up to €20,000,000 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. In addition, violations of Belgian privacy and data protection law may result in civil action for damages.

Scope

5 Exempt sectors and institutions

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 PII by all types of organisations in all sectors. That being said, certain types of PII processing are (partially) exempted or subject to specific rules, including the processing of PII:

- 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 (such as the Standing Policy Monitoring Committee and the Standing Intelligence Agencies Review Committee).

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The GDPR and the Bill generally apply to the processing of PII in connection with the interception of communications and electronic marketing, as well as monitoring and surveillance of individuals. In addition, these topics are addressed by specific laws and regulations, including:

- the Belgian Criminal Code, the Electronic Communications Act and 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, and the Royal Decree of 4 April 2003 regarding spam (electronic marketing); and
- the Belgian Act of 21 March 2007 on surveillance cameras, the Royal Decree of 10 February 2008 regarding the signalling of camera surveillance, 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 the Collective Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance in the workplace (surveillance of individuals).

7 Other laws

Identify 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 commincations 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.

8 PII formats

What forms of PII are covered by the law?

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

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Belgian data protection law applies to processing of PII carried out in the context of the activities of an establishment of a controller or processor in Belgium. In addition, Belgian data protection law can also apply to the processing of PII by organisations that are established outside the EU. This is the case where such organisations process PII of individuals located in Belgium in relation to:

- 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 PII 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 case, the data protection law of the member state where the controller is established will apply.

10 Covered uses of PII

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

In principle, all types of PII processing fall within the ambit of Belgian data protection law, regardless of who is 'controlling' the processing or merely processing PII 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 PII. Controllers can engage a 'processor' to carry out PII 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 PII only on the controller's instructions, keep internal records of PII 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 PII

11 Legitimate processing – grounds

Does the law require that the holding of PII 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 PII processing activity. The exhaustive list of potential legal grounds for processing of PII set forth in the GDPR will be available to controllers that are subject to Belgian data protection law:

- the data subject has unambiguously consented to the processing of his or her PII;
- the 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;
- the processing is necessary for compliance with a legal obligation under EU or member state law to which the controller is subject;
- the processing is necessary in order 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 in 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 PII 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 PII, more restrictive requirements in terms of legal bases apply (see question 12). Furthermore, controllers that rely on consent to legitimise the processing of PII 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.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The processing of sensitive PII 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 his or her 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 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, and solely relates to the member or former members of the organisation or to persons that have regular contact with the organisation and the PII is not disclosed to third parties without the data subjects' consent;
- the processing relates to PII 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 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 on the basis of EU or member state law or pursuant 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 on the basis of EU or 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 member state law.

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

Furthermore, the GDPR and the Bill prohibit the processing of PII relating to criminal convictions and offences or related security measures, except where the processing is carried out:

- under the supervision of an official authority;
- by natural persons, private or public legal persons for managing their own litigation;
- by lawyers or other legal advisors, 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 which are determined by EU or member state law; or
- because the processing is required for scientific, historical or statistical research or archiving.

The Bill also sets forth a number of specific measures that must be implemented when processing genetic, biometric, health or PII 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 with respect to the processing of the data, must be maintained. This list must be made available to the DPA upon request. Furthermore, 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 PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Controllers are required to provide notice to data subjects whose PII they process. If PII 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 PII 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 PII processing for direct marketing purposes;
- the (categories of) recipients of PII;
- 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 the means by which 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 PII or the restriction of processing of PII 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 his or her PII;
- the right to lodge a complaint with a supervisory authority;
- whether providing the PII 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 PII and the possible consequences of the failure to provide the PII; 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 PII is not obtained directly from the data subject, the controller must provide, in addition to the information listed above, the categories of PII concerned and the source from which the PII originates. This information must be provided within a reasonable period after obtaining the PII (within one month at the latest), or when PII is shared with a third party, at the very latest when the PII is first disclosed or when the PII is used to communicate with the data subject at the latest at the time of the first communication.

14 Exemption from notification

When is notice not required?

Notice is not required if data subjects have already received the information mentioned in question 13. In addition, in cases where PII 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 PII 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
- PII must remain confidential subject to an obligation of professional secrecy regulated by EU or member state law.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Belgian data protection law includes a number of rights aimed at enabling data subjects to exercise choice and control over the use of their PII. In particular, data subjects are entitled to:

- request the controller to provide information regarding the processing of their PII and a copy of the PII being processed;
- obtain the rectification of incorrect PII relating to them and to have incomplete PII completed;
- obtain the erasure of their PII;
- obtain the restriction of the processing of their PII;
- receive the PII they have provided to the controller in a structured, commonly used and machine-readable format and to have it transmitted directly to another controller where technically feasible;
- object to the processing of their PII, for reasons related to their particular situation, if such processing is based on the ground that it 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 on the basis of the legitimate interests ground, unless the controller demonstrates that it has compelling legitimate grounds that outweigh the interests, rights and freedoms of the data subject or the processing is necessary for the establishment, exercise or defence of legal claims;
- object to the processing of their PII for direct marketing purposes; and
- not be subject to decisions having legal effects or similarly significantly affecting them, which are taken purely on the basis of automatic PII processing, including profiling.

The above mentioned data protection rights are not absolute and typically subject to conditions and exemptions set forth in the GDPR and the Bill.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

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

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Controllers are required to limit the processing of PII to what is strictly necessary for the processing purposes. In terms of data retention requirements, PII must not be kept in an identifiable form for longer than necessary in light of the purposes for which the PII is collected or further processed. This means that, if a controller no longer has a need to identify data subjects for the purposes for which the PII was initially collected or further processed, the PII should be erased or anonymised.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

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

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

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

Security

20 Security obligations

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

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

These measures must ensure an appropriate level of security 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 varying likelihood and severity for the rights and freedoms of individuals.

These measures may include:
- the pseudonymisation and encryption of PII;
- 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 PII in a timely manner 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 PII and the higher the risks for the data subject, the more precautions have to be taken. The Bill, 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 PII are under appropriate confidentiality obligations.

21 Notification of data breach

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 imposes a duty on providers of publicly available electronic communications services to notify security breaches, under certain conditions, to the 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 to mitigate 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 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. In addition, data subjects must be informed without undue delay when the security breach is likely to adversely affect their privacy or PII.

As of 25 May 2018, 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 PII 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 PII 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 disproportionate effort. In the latter case, a 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 PII without undue delay. In Belgium, data breaches can be notified to the DPA via an online form made available on the DPA's website. The DPA is in the process of updating the existing form in light of the data breach notification requirements under the GDPR, but in the meantime controllers can continue to use the existing form.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

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 PII on a large scale.

In addition, the Bill provides that the appointment of a data protection officer is required for:
- private organisations that process PII on behalf of a public authority (as data processors) or that receive PII from a public authority and the processing of such PII is considered to present a high risk; and
- controllers processing PII for archiving purposes in the public interest or for 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, the GDPR and the controller's or processor's policies, including with respect to the assignment of responsibilities, raising awareness and training the controller's or processor's personnel involved in the processing of PII;
- assist with data protection impact assessments; and
- act as contact point for the data subjects and the relevant supervisory authorities.

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

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

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

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 PII;
- the categories of data recipients, including recipients in third countries;
- transfers of PII 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 PII 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 PII to third countries, including the identification of such countries and, where applicable, documentation of the safeguards put in place to protect the PII 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 PII 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 PII or PII relating to criminal convictions and offences.

24 New processing regulations

Are there any obligations in relation to new processing operations?

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 in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR. When doing so, controllers must take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing. Privacy by default means that controllers must implement appropriate technical and organisational measures to ensure that, by default, only PII that is strictly necessary for each processing purpose is processed.

When engaging in new PII 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 PII processing activities triggering the requirement to conduct a data protection impact assessment include:
- automated individual decision-making;
- large-scale processing of sensitive PII or PII 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 processing would result in a high risk and no measures are taken by the controller to mitigate such risk, the controller must consult the DPA prior to commencing the envisaged PII processing activity. The Bill excludes, under certain conditions, processing activities for journalistic, academic, artistic or literary purposes from such requirement.

The DPA has 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. The Recommendation also includes a list of PII processing activities that require a data protection impact assessment and a list of PII processing activities that do not trigger the requirement to conduct a data protection impact assessment.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

As of 25 May 2018, the obligation for controllers to register their data processing activities with the DPA no longer exists. Instead, controllers and processors are required to maintain internal records of their processing activities (see question 23). However, if a controller or processor appoints a data protection officer, such appointment must be communicated to the DPA through a specific online form made available on the DPA's website.

26 Formalities

What are the formalities for registration?

See question 25.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable, see question 25.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

See question 25.

29 Public access

Is the register publicly available? How can it be accessed?

See question 25.

30 Effect of registration

Does an entry on the register have any specific legal effect?

See question 25.

31 Other transparency duties

Are there any other public transparency duties?

No.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the 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 PII and categories of data subjects; and
- the obligations and rights of the controller.

Such agreement should stipulate that the processor:
- processes the PII only on documented instructions from the controller, unless otherwise required by EU or 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. In addition, 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 PII 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 PII;

- 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 PII, at the choice of the controller, and deletes existing copies unless further storage is required under EU or member state law; and
- makes available to the controller all information necessary to demonstrate compliance with the GDPR and contribute to audits.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

In general, there are no specific restrictions under the GDPR or the Bill on the disclosure of PII other than the restrictions resulting from the general data protection principles (such as lawfulness, notice and purpose limitation).

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

PII can be transferred freely to other countries within the EEA, as well as to countries recognised by the European Commission as providing an 'adequate level of data protection' (see http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm for a list of countries deemed to be providing an adequate level of data protection).

Transferring PII to countries outside the EEA that are not recognised as providing an 'adequate level of data protection' is prohibited unless:

- the data subject has explicitly given his or her 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 for 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 for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or other persons;
- 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; or
- 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 the purposes of 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 PII. In this case, the controller must inform the 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 PII receives an adequate level of data protection and data subjects are able to exercise their rights after the PII 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. In addition, transfers of PII can be legitimised by executing an ad hoc data transfer agreement. However, in such cases the prior authorisation of the Minister of Justice (by Royal Decree) must be obtained.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

In general, cross-border data transfers do not need to be notified to the DPA.

As mentioned in question 34, prior authorisation by the Minister of Justice is required if the controller relies on an ad hoc data transfer agreement to legitimise the transfer of PII to non-adequate countries. Such authorisation is not required when the controller has guaranteed an adequate level of data protection by executing the standard contractual clauses approved by the European Commission.

36 Further transfer

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 and authorisation requirements described in questions 34 and 35 apply regardless of whether PII is transferred to a service provider (ie, processor) or another controller.

The restrictions and requirements applicable to onward PII 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 EEA. For example, the standard contractual clauses and the EU–US Privacy Shield framework contain specific requirements for onward data transfers.

Rights of individuals

37 Access

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

Data subjects have a right to 'access' the PII that a controller holds about them. When a data subject exercises his or her 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 PII;
- the purposes for which his or her PII is processed;
- the categories of PII concerned;
- the recipients or categories of recipients to whom PII has been or will be disclosed, in particular, recipients in third countries, and in 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 PII 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 PII 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 PII; 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 PII 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 PII 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.

In addition, exemptions to the right of access apply to PII originating from certain public authorities, including the police and intelligence

Update and trends

Over the past year, the DPA has focused its efforts on preparing for the GDPR, as well as providing guidance to companies about several aspects and implications of the GDPR. The DPA also focused on big data and published its 'Report Big Data', which includes recommendations regarding the application of the GDPR to big data.

services and to PII processed for journalistic, academic, artistic or literary purposes.

38 Other rights

Do individuals have other substantive rights?

In addition to the right of access described above, data subjects have the following rights:

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

Erasure ('right to be forgotten')
Data subjects have the right to request the erasure of PII concerning them where:
- the PII 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 his or her consent and there is no other legal basis for the processing;
- the data subject objects to the processing of his or her PII 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 his or her PII for direct marketing purposes;
- PII has been unlawfully processed;
- PII has to be erased for compliance with a legal obligation under EU or member state law; and
- PII has been collected in relation to 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 member state law;
- the performance of a task carried out in the public interest or in 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 PII is restricted by the controller, where one of the following conditions applies:
- the data subject is contesting the accuracy of his or her PII, in which case, the processing should be restricted for a period enabling the verification by the controller of the accuracy of the PII;
- the processing is unlawful and the data subject opposes the erasure of the PII and requests the restriction of its use instead;
- the controller no longer needs the PII, but the PII 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 his or her PII for purposes other than direct marketing, based on grounds relating to his or her 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 PII 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 PII to pursue its legitimate interests. In addition, data subjects are in any event (ie, without any specific justification) entitled to object, at any time, to the processing of their PII for direct marketing purposes.

Data portability
Data subjects are entitled to receive in a structured, commonly used and machine-readable format the PII they have provided directly to the controller and the PII they have provided indirectly by virtue of the use of the controller's services, websites or applications. In addition, where technically feasible, data subjects have the right to have their PII transmitted by the controller to another controller. The right to data portability only applies if:
- the PII is processed on the basis of the data subject's consent or the necessity of the processing for the performance of a contract; and
- the PII is processed by automated means.

The above mentioned rights are subject to certain restrictions, in particular in the case of processing PII originating from certain public authorities, including the police and intelligence services, or processing of PII 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 with investigative, control and enforcement powers) to enforce their rights. Furthermore, 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 on the basis of 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 member state law; or
- is based on the data subject's explicit consent.

39 Compensation

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 the Belgian data protection law. Controllers will only be exempt from liability if they are able to prove that they are not responsible for the event giving rise to the damage. Individuals may choose to mandate an organ, organisation or a non-profit organisation to lodge a complaint on their behalf before the DPA or the competent judicial body.

40 Enforcement

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

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Controllers can appeal against certain decisions of the DPA's inspection service (including orders to freeze or limit processing activities, decisions to temporarily or permanently prohibit the processing or decisions to seize or seal goods or computer systems) in front of the DPA's Litigation Chamber. In addition, controllers can appeal the decisions of the DPA's Litigation Chamber in front of a specific section of the Appeal Court of Brussels (ie, *Cour des Marchés* or *Marktenhof*).

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

In general, 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 purposes of such storage or access and their rights with regard to the processing of their PII. 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 4 February 2015, the DPA issued practical guidance on the cookie consent requirements, which clarifies 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 cookie requirements under Belgian law result from the legal regime for the use of cookies set forth by the ePrivacy Directive 2002/58/EC (the ePrivacy Directive, as transposed into member state law). The ePrivacy Directive is currently under review and will most likely be replaced by the ePrivacy Regulation in the near future. The exact timing of the adoption of the ePrivacy Regulation has, however, not yet been determined.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

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 SMS) 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 his or her right to opt out from receiving future electronic marketing and provide an appropriate means to exercise this right electronically. In addition 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. Furthermore, the addressee should be able to withdraw his or her 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 (see question 43), these rules may change once the ePrivacy Directive is replaced by the ePrivacy Regulation (which has not been adopted yet).

45 Cloud services

Describe 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 case of termination of the cloud provider's business or the service contract; and
- violations of data transfer restrictions.

HUNTON ANDREWS KURTH

Aaron P Simpson **asimpson@HuntonAK.com**
David Dumont **ddumont@HuntonAK.com**
Laura Léonard **lleonard@HuntonAK.com**

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 00
Fax: +32 2 643 58 22
www.HuntonAK.com

To address these risks, the DPA has issued a number of 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, taking into account 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, taking into account the risk analysis;
- inform data subjects about the migration of their PII to the cloud; and
- monitor changes to cloud services over time and update the risk analysis in light of such changes.

Brazil

Jorge Cesa, Roberta Feiten and Conrado Steinbruck

Souto Correa Cesa Lummertz & Amaral Advogados

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Data privacy law in Brazil is a collection of principles and sector-specific laws, as there is no single comprehensive statute dedicated to regulating the subject. The Federal Constitution provides general privacy principles and rights, among which is the right to protect and seek moral and material damages arising out of the violation of one's right to privacy, private life, honour and image (personality rights). The Federal Constitution also guarantees the right to habeas data and the right of secrecy of communications, which is exempted only upon a court order rendered in connection with a criminal investigation.

Lacking a single statute, practitioners and businesses rely mostly on the provisions set forth by the Internet Act (Federal Law 12,965/2014) and its regulatory decree (Presidential Decree 8,771/2016) to ensure data protection compliance. While the Internet Act establishes general principles, rights and obligations regarding the online collection, storage, use, treatment and disclosure of personal data, the decree brings a novel definition of 'personal data' and 'reatment of personal data'.

The provisions of the Consumer Protection Code (Federal Law 8,078/1990) are also applicable to data collected or treated in connection with a consumer relationship. The statute guarantees some privacy rights, such as the right to access and correct data pertaining to consumers.

There are also some data protection provisions in the Positive Credit Act (Federal Law 12,414/2011), which authorises the creation of databases containing information on the data subjects' credit history, but expressly prohibits the inclusion in such databases of sensitive (that is, pertaining to one's social origin, ethnicity, health, genetic information, sexual orientation or political, religious or philosophical convictions) or excessive (that is, not related to credit scoring) information.

Regarding personal data collected, stored and treated by public entities or publicly funded private entities, the Information Access Act (Federal Law 12,527/2011) contains specific provisions restricting the disclosure of such types of data.

It is important to point out that the Brazilian Congress passed in July 2018 a bill of law (PL 4,060/2012, redocketed in the Senate as PLC 53/2018) establishing a single Data Protection Statute (DPS). The bill was remitted to the President, who has until early August to sanction or veto it.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no data protection authority in Brazil. However, there are several entities with standing to enforce administratively and judicially consumer and privacy law, including, inter alia, the Federal and State Prosecution Services, the Ministry of Justice's National Consumer Secretariat and the state's Consumer Protection and Orientation State Programme (PROCON) and Public Defender's Offices.

Nonetheless, it is important to highlight that Presidential Decree 8,771/2016 determines the Internet Steering Committee to promote studies and propose recommendations, norms and technical standards to ensure data security by internet access providers and online service providers.

The Presidential Decree also establishes that the overseeing and enforcement of the Internet Act and its regulatory decree will be conducted by three entities. The National Telecommunications Agency (ANATEL) is responsible for infringements related to the Telecommunications Act (Federal Law 9,472/1997), the National Consumer Secretariat will follow on consumer rights violations and the Administrative Council for Economic Defence (CADE) will oversee infractions with reflexes on competition law.

3 Legal obligations of data protection authority

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

The Presidential Decree regulating the Internet Act establishes that the federal entities with standing to enforce their rules shall collaborate with each other and observe the guidelines established by the Internet Steering Committee.

It is noteworthy that most entities with standing to enforce data privacy rules are independent and normally act individually, simultaneously conducting their own investigations and enforcing their own understanding of the law.

4 Breaches of data protection

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

Non-compliance with the data privacy provisions of the Internet Act can lead to administrative sanctions without prejudice to any other applicable civil, administrative or criminal sanctions. According to article 12 of the Internet Act, the following administrative sanctions can apply individually or cumulatively:

- a warning indicating a deadline to adopt corrective measures;
- fine of up to 10 per cent of the gross income of the economic group in Brazil in the last fiscal year, excluding taxes, and considering the economic condition of the infringer, the principle of proportionality between the gravity of the breach and the size of the penalty;
- the temporary suspension of the activities that entail the collection, storage, keeping and treatment of records, personal data or communications; or
- the prohibition of the execution of activities that entail the collection, storage, keeping and treatment of records, personal data or communications.

It is worth noting that if the breach is committed by a foreign company, the Brazilian subsidiary is jointly liable for the payment of the fine.

In addition, if the data subject whose data was breached or misused is a consumer, then the administrative sanctions established by the Consumer Protection Code may also apply, which include, inter alia:

- warnings;
- payment of penalties of up to 3,000,000 Fiscal Reference Units, which no longer exist, but are monetary adjusted and can surpass US$2.5 million;
- temporary suspension of the activity;
- administrative intervention; and
- publication of public notices.

The Consumer Protection Code also considers as criminal offences the acts of denying or hindering consumer access to the information contained in records, databases and files, as well as the failure to immediately rectify any consumer information contained in records, databases and files that he or she knows or should have known to be inaccurate.

Deliberate and unauthorised disclosure of data can also amount to crimes of disclosure of secrets and violations of professional secrecy, while unconsented hacking of a computer device to obtain, alter or destroy data or information is also considered a crime as set forth in the Criminal Code (Federal Decree-Law 2,848/1940).

Deliberate and unauthorised disclosure of financial operations and services by financial institutions are a criminal offence set forth by the Bank Secrecy Act (Federal Complementary Law 105/2001), while the unauthorised interception of communications data or disclosing such data obtained by means of a court order also amount to crimes, as per the Communications Intercept Act (Federal Law 9,296/1996).

Scope

5 Exempt sectors and institutions

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

There are no exempt sectors or institutions.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Communications Intercept Act (Federal Law 9,296/1996) and the Bank Secrecy Act (Federal Complementary Law 105/2001) have some provisions regarding access to communications and financial data respectively.

Law enforcement agencies have extrajudicial authority to request information pertaining to one's 'individual qualification, parents' names and address', as established by the Internet Act, the Money Laundering Act (Federal Law 9,613/98) and the Criminal Organisation Act (Federal Law 12,850/2013).

There is no specific law regulating electronic marketing; the Consumer Protection Code has some provisions regulating general marketing and offering of products and services, but no specific data protection provision on marketing.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Besides the statutes mentioned above, there are other relevant statutes containing privacy provisions. The most relevant ones are:

- the Civil Code (Federal Law 10,406/2002), implementing some of the principles and rights established in the Federal Constitution, among which are personality rights, including the right to privacy and the protection of one's name, image and likeness (rights of publicity);
- the Positive Credit Act (Federal Law 12,414/2011), authorising the creation of databases containing information on the data subjects' credit history, but expressly prohibiting the inclusion in such databases of sensitive (that is, pertaining to one's social origin, ethnicity, health, genetic information, sexual orientation or political, religious or philosophical convictions) or excessive (that is, not related to credit scoring) information;
- the Information Access Act (Federal Law 12,527/2011), governing access to information held by public entities or publicly funded private entities. This law has some provisions regulating the disclosure of personal data to third parties;
- the Habeas Data Act (Federal Law 9,507/1997), regulating the procurement pertaining to the writ of habeas data;
- the National Tax Code (Federal Law 5,5172/1996), prohibiting the disclosure of tax records and financial information of taxpayers by the Treasury;
- the Money Laundering Act (Federal Law 9,613/98) and the Criminal Organisations Act (Federal Law 12,850/2013) grant law enforcement agencies extrajudicial authority to request information pertaining to one's 'personal qualification, parents' names and address'. The Criminal Organisations Act also establishes that, for a period of five years, transport companies must retain travel and booking logs, while landline and mobile phone companies must retain logs on local, long distance and international telephone calls;
- the Telecommunications Act (Federal Law 9,472/1997), generically stating that telecommunications users have the right to privacy and communication secrecy;
- Ordinance 589/2015 issued by the Ministry of Health, regulating the National Policy for Computerised Health Information, and Ordinance 2,073/2011 issued by the Ministry of Health, regulating the standards used to share information within the public healthcare system, have generic provisions on patient privacy;
- Normative Resolution 124/2006 issued by the National Supplementary Health Agency, establishing a fine of 50,000 Brazilian reais to healthcare insurance companies for the unauthorised disclosure of consumers' health conditions; and
- Federal Decree 8,789/2016, determining the sharing of databases held by federal entities containing inter alia personal data, corporate data and labour data in order to streamline the rendering of public services.

There are also other federal, state and municipal statutes containing data privacy provisions or regulating the use of personal data.

8 PII formats

What forms of PII are covered by the law?

Personal identifiable information is protected irrespective of the format or medium in which it is stored.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The Internet Act expressly states that Brazilian privacy law applies whenever data is collected, stored, kept or treated in Brazil, or if goods and services are offered to the Brazilian public. So, even if the data is collected or treated by foreign entities, Brazilian law still applies.

10 Covered uses of PII

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

Data owners, controllers and processors are not treated differently, but concrete circumstances may impose additional obligations or treatment on any of them.

Legitimate processing of PII

11 Legitimate processing – grounds

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

Free, informed and express consent of the data subject is required prior to the collection, use, processing, transfer and disclosure of personal data, irrespective of the purpose of such actions.

There is no specific format regarding the way that consent is given; it could be verbal, written or by ticking a box, if given online. Nonetheless, written consent in Portuguese is recommended in case of adjudication.

Before consenting, the data subject should receive conspicuous and complete information on:

- the types of data collected;
- purposes for which the data is collected, used, stored and treated;
- conditions under which it may be disclosed to third parties; and
- means employed to protect it.

Consent is limited to the types of data and purposes specified in the expressly consented to by the data subject, so fresh consent is required for the collection of other data or uses for other purposes.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

There are some sector-specific laws and regulations that treat specific types of PII differently.

For instance, the Positive Credit Act authorises the creation of databases containing information on the data subjects' credit history, but expressly prohibits the inclusion in such databases of sensitive (that is, pertaining to one's social origin, ethnicity, health, genetic information, sexual orientation or political, religious or philosophical convictions) or excessive (that is, not related to credit scoring) information.

The Consumer Protection Code also treats 'negative data' differently, as it prohibits the storing of negative data in databases for more than five years.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

As a general rule, notification is not required when the data subject has consented to the collection of the PII.

The Consumer Protection Code also states that whenever a new file or record is created pertaining to a consumer, he or she will be notified in writing, except if the consumer had requested the creation of such file or record.

14 Exemption from notification

When is notice not required?

Notice is not required when the data is volunteered by the data subject. Data controllers who disclose data upon receipt of court orders can also be ordered not to inform the data subject of the data disclosure.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

There is no explicit provision granting data subjects control of the use of their information by owners of PII. However, such a right is implied in two scenarios. One is when the data subject gives consent to the collection and treatment of PII for the specific activities listed in the consent document.

The other scenario is by exercising the right to revoke consent, at any time, partially or entirely, for any data collection and processing activities, thus enabling the data subject some control over the use of his or her personal data.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Consumer data and data pertaining to positive credit databases must be objective, clear, true and easily comprehensible. In addition, data subjects may ask data controllers to rectify any inaccurate data.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The Presidential Decree regulating the Internet Act establishes that internet access providers and online service providers must retain the least amount of personal data, private communications and connection and access logs as possible. Such data must be excluded as soon as its use has fulfilled its purpose or when the legal data retention period has ended.

The legal retention period is set by the Internet Act and applies to connection logs (which must be retained by internet access providers for one year) and access logs (which must be retained by online service providers for six months). The Criminal Organisations Act also establishes that, for a period of five years, transport companies must retain travel and booking logs, while landline and mobile phone companies must retain logs on local, long distance and international telephone calls.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

PII can only be used for the specific purposes consented to by the data subject. Any processing of PII that the data subject has not consented to is likely to be deemed misuse of PII. In addition, the Internet Act restricts the use of PII to the finalities that:

- justify its collection;
- are not prohibited by legislation; and
- are specified in the service agreements or terms of use of online service providers.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

There are no exemptions to the finality principle. Any collection and treatment of PII must be consented to by the data subject. If the data controller intends to use the PII for purposes outside the scope of the original consent, fresh consent is required.

Security

20 Security obligations

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

The Presidential Decree regulating the Internet Act provides for a number of security measures to keep PII safe, including:

- control of access to the personal data by authorised personnel;
- two-factor authentication and other authentication mechanisms to individualise the employee accessing or treating the data;
- creation of a detailed access log, containing the time, duration, identification of the person accessing the data and the files accessed; and
- use of encryption or other measures to keep the data safe.

In addition, it also attributes to the Internet Steering Committee the obligation to promote studies and propose recommendations, norms and technical standards to ensure data security by internet access providers and online service providers, and determines that information on the security standards adopted by internet access providers and online service providers be published on their websites.

21 Notification of data breach

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 specific provision establishing a data breach notification duty. However, such a notification is expected by virtue of general transparency and good-faith principles.

Update and trends

The Brazilian Congress passed in July 2018 a bill of law (PL 4,060/2012, redocketed in the Senate as PLC 53/2018) establishing a single Data Protection Statute (DPS). The bill was remitted to the President, who has until early August to sanction or veto it.

Although both houses of Congress were working on their own version of a DPS for years, recent international scandals on the misuse of personal data, data breaches and pressure by think tanks and non-governmental organisations have motivated legislators to speed up the analysis and assign urgency to their respective bills.

PLC 53/2018 has benefited from several public hearings and was largely inspired by the EU's General Data Protection Regulation, being similar to the European legislation in many topics, such as:

- the establishment of an independent supervisory authority;
- the prohibition of the collection and treatment of personal data without the express consent of the data subject, thus prohibiting the 'opt-out model';
- restrictions on the international transfer of personal data;
- compulsory notices in case of data breaches; and
- special consent to process sensitive data, among other topics.

It is noteworthy that the DPS establishes the creation of the National Data Protection Authority (NDPA) and assigns it the responsibility to regulate various matters not expressly covered by the DPS, to inspect the application of the DPS and to impose sanctions in cases of non-compliance. The sanctions established by the DPS range from simple warnings to more severe penalties, such as, inter alia:

- simple or daily fines of up to 2 per cent of the last fiscal year's gross revenue in Brazil, limited to 50 million reais per infringement act;
- the obligation to inform the public of applied sanctions; and
- prohibition of personal data treatment activities.

It is worth noting that despite the lack of a single data protection statute in Brazil, the level of awareness has been increasing in recent years, especially within consumer protection bodies. In April 2018, the Prosecution Service of the Federal District and Territories created a personal data protection commission, seeking to receive complaints, investigate abuses and breaches and enforce the applicable rules.

In addition, if the data is collected or treated as a result of a consumer relationship, it is possible to reason by analogy the applicability of the Consumer Protection Code provision that obligates suppliers of goods and services to disclose to the public through paid advertising any fact that may risk the consumer's health or safety.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

There is no obligation to appoint a data protection officer.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Owners and processors of PII are required to observe the legal data retention periods, as well as the security obligations mentioned above.

It is also highly advisable to maintain records of the consent given by data subjects for evidentiary purposes.

24 New processing regulations

Are there any obligations in relation to new processing operations?

There are no specific regulations on this matter.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There is no registration obligation as there is no data protection authority in Brazil. However, sector-specific supervisory authorities may impose such an obligation on their supervisees.

26 Formalities

What are the formalities for registration?

There are no formalities as there is no registration obligation.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There are no penalties as there is no registration obligation.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

The Presidential Decree regulating the Internet Act determines that information on the security standards adopted by internet access providers and online service providers be published on their websites.

Also, although there is no specific provision establishing a data breach notification duty, general transparency and good-faith principles require the issuance of a public notice informing the affected parties of a breach.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

There is no specific provision regulating the transfer of PII to outsourced processing services. Nonetheless, as the Internet Act prohibits the transfer of PII and connection and access logs to any third parties without free, express and informed consent, it is advisable to obtain consent in order to outsource processing activities.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

PII must not be disclosed to third parties without a court order or the free, express and informed consent of the data subject. Law enforcement agencies have the right to access one's 'personal qualification, parents' names and address' without the need for a court order.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

There are no restrictions on the cross-border transfer of PII. Nonetheless, it is worth noticing that the Consumer Protection Code

subjects all suppliers in the supply chain of a service or product to a strict liability standard, so it is possible to reason by analogy to hold transferors and transferees liable for the misuse or lack of consent on the collection, treatment or transfer of PII.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

As there is no supervisory authority, there is no need to notify or obtain authorisation.

36 Further transfer

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 restrictions on the further transfer of PII provided that the data subject has given free, express and informed consent to transfer PII to third parties.

Rights of individuals

37 Access

Do individuals have the right to access their personal information held by PII 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 information held by PII owners by means of a simple extrajudicial request. It is noteworthy that denying or hindering access to such data is considered a criminal offence by the Consumer Protection Code.

Data subjects can also rely on the writ of habeas data and on the Information Access Act to obtain access to their PII depending on the circumstances of the denial.

38 Other rights

Do individuals have other substantive rights?

Data subjects have the right, at any time, to withdraw consent, obtain information on the stored data and request its rectification.

39 Compensation

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?

Individual data subjects whose data has been misused or breached may seek compensation for moral and material damages. While material damages must be evidenced, moral damages arising out of personality and privacy rights violations are deemed to be presumed.

Data subjects can seek compensation by bringing individual lawsuits or by enforcing a favourable decision on the merits rendered in a class action.

40 Enforcement

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

Data subjects can enforce their own rights directly through the judicial system and by seeking the assistance of a consumer protection entity.

In addition, as mentioned in question 2, there are several entities with standing to enforce consumer and privacy law administratively and judicially, including, inter alia, the Federal and State Prosecution Services, the Ministry of Justice's National Consumer Secretariat and the state's PROCON and Public Defender's Offices.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

There are no other exemptions or restrictions.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

As there is no data protection supervisory authority, there is no decision to be adjudicated.

However, it is worth mentioning that any administrative fine or penalty applied by any of the several entities with authority to enforce collective data privacy rights (such as PROCONs or the Ministry of Justice's National Consumer Secretariat) are subject to second instance administrative review and judicial review by challenging the legality of the administrative decision.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Although the Internet Act and its regulatory decree contain several data protection provisions, none is specific to the use of 'cookies'.

Souto Correa
Cesa Lummertz
& Amaral Advogados

Jorge Cesa **jorge.cesa@soutocorrea.com.br**
Roberta Feiten **roberta.feiten@soutocorrea.com.br**
Conrado Steinbruck **conrado.steinbruck@soutocorrea.com.br**

Av Carlos Gomes, 700, 13º andar
CEP: 90.480-000,
Porto Alegre, RS
Brazil

Tel: +55 51 3018 0500
Fax: +55 51 3018 0500
www.soutocorrea.com.br

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

There are some state laws regulating marketing by email and telephone. For instance, Rio de Janeiro State enacted State Law 6,161/2012, regulating group buying websites within Rio de Janeiro. This law limits email marketing to consumers who have expressly consented to receive such emails.

Despite the above, it is important to highlight that sending unsolicited promotional and marketing emails is widely accepted in Brazil. In fact, there are some precedents by the Superior Court of Justice and some state courts of appeals finding that the receipt of unsolicited marketing emails does not amount to moral damages.

As to telephone marketing, some states have enacted do-not-call laws creating a register of telephone numbers, the calling of which is prohibited under payment of fines.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific provisions regulating cloud services.

Chile

Claudio Magliona, Nicolás Yuraszeck and Carlos Araya

García Magliona & Cía Abogados

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments 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 the respect and protection of privacy and honour of the person and his or her family at a constitutional level. 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 OECD guidelines, Directive 95/46/EC, EU General Data Protection Regulation or the European Convention on Human Rights and Fundamental Freedoms).

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

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.

3 Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with 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 the Congress that will reform the whole data protection environment in the country and will create the first data protection authority in Chile.

4 Breaches of data protection

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 US$75 to US$760, or from US$760 to US$3,800 if the breach comes from financial data). 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 the civil judge, considering the circumstances of the case and the relevance of the facts.

Scope

5 Exempt sectors and institutions

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

The Law applies to both private and public sector organisations and agencies. However, regarding public sector organisations, there are some special rules for 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. In addition, regarding public sector organisations, individuals may only exercise the right of information, not the right to modify information.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

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).

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

In addition to the laws set forth above, there are numerous other laws that address privacy issues, for example:

- Law No. 20,584, which contains provisions regarding the privacy of medical records along with the same 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 access on occasion of the employment relationship. In addition, 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.

8 PII formats

What forms of PII 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.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The Law does not contain an explicit provision in this respect; however, taking into account the other provisions of the Law, its reach is limited to data owners and data processors established or operating in the Chilean jurisdiction.

10 Covered uses of PII

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

Yes, all processing of PII is covered. 'Data processing' is broadly defined in the Law as any operation or set of technical operations or procedures, automated or not, that make 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 PII and those who provide PII 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 PII

11 Legitimate processing – grounds

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

Yes, 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 in order 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; and
  - 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. In any case, the information must be exact, updated and respond truthfully to the real situation of the subject of the data.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Yes. The Law imposes more stringent rules with regard to sensitive data, which is defined as that which refers to the physical or moral characteristics of persons or to 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 PII 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. Whoever discloses such content improperly shall be punished with a high financial penalty of between approximately 45,000 and 450,000 Chilean pesos.

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 PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

No, the Law does not require owners of PII 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.

14 Exemption from notification

When is notice not required?

Despite the fact that notice is not required, as mentioned, authorisation is 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.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Yes, at two levels. First, at the moment of gathering the data because the general rule is that authorisation is required; and second, after the data is gathered, individuals have the right of information, the right of modification and right of cancellation, among others.

In addition, individuals are entitled to demand information about data concerning themselves, 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.

If the personal data is erroneous, inexact, equivocal or incomplete, and such situation has been evidenced, the individual shall have the right to have it amended.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

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.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes, the Law does restrict the length of time PII 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. So, if the data has expired, it must be eliminated.

In addition, personal data related to 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.

As regards 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 elapsed, or after the sanction or penalty has been served.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes. As previously stated, 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.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

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.

Security

20 Security obligations

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

The Law does not impose any type of security measures that data owners and entities must take in relation to PII. 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 data of their clients and their wire transfers, in which encryption is mandatory.

21 Notification of data breach

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

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

No. There is no data protection officer in Chile.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

No, owners or processors of PII 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.

24 New processing regulations

Are there any obligations in relation to new processing operations?

No, currently there are no obligations in relation to new processing operations.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

No. There are no registration requirements for data-processing activities in Chile. However, as previously mentioned, the Service of Civil Registration and Identification shall keep a record of personal data banks managed by government agencies.

Update and trends

The Chilean government sent a Bill to the Congress that seeks to amend the current legislation on personal data, updating it and adapting it with OECD standards. The main aspects that the Bill seeks to introduce in the Chilean legislation are, among others: the express recognition of principles such as finality, proportionality, quality, security, liability and legality of data processing; a more accurate definition of 'consent' as the main source of the legitimacy of data processing and a new statute of exceptions for consent; the creation of a data protection authority (the Personal Data Protection Agency); the establishment of new proceedings to prosecute liabilities; and many other modifications. The Bill is currently in its first constitutional stage in the Congress.

On 8 May 2018, the Congress approved, in the second constitutional stage, a Bill that modifies the Chilean Constitution. A new paragraph is to be incorporated into the Chilean Constitution that enshrines respect and protection of the private life and honour of the individual and his or her family, recognising the protection of their personal data, in the manner and under the conditions determined by the respective law. It is now up to the executive branch to approve, promulgate and publish the Bill already approved.

26 Formalities

What are the formalities for registration?

As previously stated, there is no registration process for private entities. 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. In this case, there is no fee payable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There is no registration process for private entities in Chile.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

There is no registration process for private entities in Chile.

29 Public access

Is the register publicly available? How can it be accessed?

Regarding personal data processing by government agencies, this record shall be public. The Law does not contemplate how it can be accessed as a public record.

30 Effect of registration

Does an entry on the register have any specific legal effect?

No. The Law does not establish any specific legal effect for entry on the register maintained by the Service of Civil Registration and Identification for personal data banks managed by government agencies.

31 Other transparency duties

Are there any other public transparency duties?

No, currently the Law does not contemplate any public transparency duty.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

At present, 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 the exceptions mentioned in question 14.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

There are no further restrictions on the disclosure of PII 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.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

At present, the Law does not contain a specific provision in this respect. However, the transfer of PII outside the jurisdiction is considered as a use of data, and will require authorisation.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

At present, the Law does not contain a specific provision in this respect.

36 Further transfer

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

At present, 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 above.

Rights of individuals

37 Access

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

Yes. According to 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.

In order to exercise the right to access, the data subject must address to 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 by means of any act or agreement, with the exception of 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.

38 Other rights

Do individuals have other substantive rights?

Yes. In addition to the right to information or access, the Law also provides individuals the following rights:

- 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;
- 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;
- 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;
- 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
- right of opposition: the subject may oppose the use of his or her personal data for purposes of advertising, market research or opinion polls.

39 Compensation

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. As mentioned in question 4, 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 in order to be entitled to monetary damages or compensation.

40 Enforcement

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

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

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.

In addition, the Law 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.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes. A final judgment issued by the general courts of Chile regarding the procedure briefly described in question 37 may be appealed to the respective court of appeals.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

At present, 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 exceptions mentioned in question 14.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

As previously stated, 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. In addition, Law No. 19,496 on the Protection of Consumer Rights contains a provision regarding marketing by email (also known as '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

GARCÍA MAGLIONA & CIA
ABOGADOS

Claudio Magliona **cmagliona@garciamagliona.cl**
Nicolás Yuraszeck **nyuraszeck@garciamagliona.cl**
Carlos Araya **caraya@garciamagliona.cl**

La Bolsa 81, 6th floor
Santiago
Chile

Tel: +56 2 377 9450
Fax: +56 2 2377 9451
www.garciamagliona.cl

messaging services shall indicate an expedited way that the addressees may request the suspension thereof.

45 Cloud services

Describe 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 make 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 of between approximately US$75 to US$760, as well as the high risk of litigation (fines are viewed and determined in a summary procedure). In addition, 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

China

Vincent Zhang and John Bolin
Jincheng Tongda & Neal

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legal framework governing the protection of PII in the People's Republic of China (the PRC, or China) is undergoing rapid development. No single overarching data protection law has been promulgated. Instead, data protection-related legal provisions are distributed among various laws, regulations, implementing measures and other guidance, including industrial sector-specific rules and industrial standards. In China, laws are generally promulgated by the highest legislative organ of the state, while regulations and other implementing measures are promulgated by the State Council (the highest administrative organ) and designated administrative authorities.

The PRC's legal framework for data protection is principally encompassed by the umbrella laws listed below.

- The Decision on Strengthening the Protection of Online Information, promulgated by the Standing Committee of the National People's Congress (effective 28 December 2012, the 2012 NPC Network Decision), which codifies several essential principles of PII protection, establishing a general framework which has since supported the development of more detailed laws and regulations.
- The General Provisions of the Civil Law (effective 1 October 2017, the Civil Law), which recognises an individual's rights over personal information as constituting fundamental civil rights.
- The Tort Liability Law (effective 1 July 2010), which accords tort liability for infringement on the privacy rights of PRC citizens.
- The Criminal Law, in particular the 7th and 9th Amendments (effective from 28 February 2009 and 1 November 2015 respectively), which imposes criminal penalties on individuals or organisations for certain violations of data protection laws and regulations, encompassing infringement on PII.
- The Cyber Security Law (effective 1 June 2017), which consolidates data protection provisions previously distributed among different rules, as well as imposing new protection requirements such as security assessments for transfers of personal information outside of the PRC.

In addition to the key laws described above, certain national technical standards also furnish relevant guidance. The most influential of such standards include the Information Security Technology – Guidelines for Personal Information Protection within Information System for Public and Commercial Services (effective 1 February 2013, the Data Protection Guidelines) (GB/Z 28828-2012); and the Information Security Technology – Personal Information Security Specifications (GB/T 3527302017) (effective 1 May 2018, the PI Security Specifications), each of which comprises non-mandatory, national-level technical standards governing personal information processing activities of an individual or organisation that oversees personal information administration, and which may be relied upon by any Chinese governmental authority when evaluating the preparedness and performance of a company that handles the PII of a PRC citizen. In essence, these guidelines furnish non-binding recommended best practices and managerial and technical standards.

Other laws and regulations, including industrial sector-specific rules in sectors such as banking and finance, consumer protection, credit reporting, healthcare, postal and courier services, telecommunications and the internet, etc, provide relevant guidance to subject individuals and organisations. (See question 7 for an indicative listing of such additional relevant rules.)

Data protection laws in China may be informed by international dialogues on privacy and data protection such as the Asia-Pacific Economic (APEC) Privacy Framework, but are not directly founded on such, accommodating other national imperatives such as state security, in addition to the protection of personal privacy, as key objectives.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no single regulatory authority in China that exercises sole responsibility for the oversight of China's data protection law. Broadly speaking, legal authority is divided into criminal and administrative components.

With respect to the criminal legal component, the Ministry of Public Security (the MPS) is the primary law enforcement agency responsible for the investigation of instances where an alleged infringement of PII may involve criminal culpability.

With respect to the administrative legal component, power is allocated among competent authorities or industry-specific regulators, who are assigned responsibility for the regulation of specific industrial sectors. The Cyberspace Administration of China (the CAC), established in 2011, is assigned general responsibility for overseeing cybersecurity protection, including data protection matters, in conjunction with other relevant authorities, including the administrations listed below.

- The China Banking and Insurance Regulatory Commission (the CBIRC). In early 2018, the PRC launched a governmental authority reorganisation reform involving 40 central departments. Pursuant to this reform, the China Insurance Regulatory Commission (the CIRC), the insurance industry regulator, merged with the China Banking Regulatory Commission (the CBRC), the banking industry regulator, together forming a new central regulator, the CBIRC, which is a ministerial-level agency of the central government of the PRC. The CBIRC is supported by the People's Bank of China (the PBOC), which will exercise responsibility for formulating major laws and regulations and basic prudential regulations for the banking and insurance industries. For an interim period until the CBIRC is fully functional, which is expected to occur in late 2018, the original departments under the CIRC and the CBRC will continue to function.
- The State Market Regulatory Administration (the SMRA). Also in early 2018, the State Administration for Industry and Commerce (the SAIC), General Administration of Quality Supervision, Inspection and Quarantine (the AQSIQ) and certain other relevant

authorities combined to form the SMRA, which is charged with responsibility for the protection of consumers' rights, including rights in PII.
- The Ministry of Industry and Information Technology (the MIIT), which oversees the telecommunications, information technology (IT) and other major industrial sectors.

Such authorities are delegated power to regulate and supervise organisations in the relevant sector, and are also invested with the power to investigate non-compliance with data protection obligations.

3 Legal obligations of data protection authority

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

There is no single regulatory authority in China that exercises responsibility for the oversight of China's data protection law. Among the administrative authorities, the CAC is responsible for coordinating with other authorities (the CBIRC, the PBOC, the SMRA, the MIIT, etc) to oversee and manage network security and data protection matters. However, there is no legal obligation for a government authority to cooperate with another for data protection matters. Further regulations and enforcement practices may likely provide more clarity on the division of authority and cooperation among the various authorities.

4 Breaches of data protection

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

Organisations and individuals who fail to comply with data protection laws may be subject to investigation, administrative sanctions and civil actions and, in the case of an infraction with serious consequences, criminal penalties.

Administrative sanctions are identified in the specific rules promulgated and implemented by the competent authorities or industry-specific regulators. For example, in the telecommunications sector, if a telecommunications service operator collects PII without consent from the individual, then the MIIT may issue a warning or an order for remediation, and may impose a fine of between 10,000 and 30,000 yuan. In the consumer protection context, if a business operator infringes on the PII of consumers, then the SMRA may issue a warning or an order for remediation, confiscate illegal gains, impose a fine or revoke the operator's business licence.

Criminal sanctions are specified in the PRC Criminal Law, which prohibits acts such as the illegal sale or provision of PII, as well as the theft or unlawful receipt of PII (whether through purchase, exchange or other means).

Scope

5 Exempt sectors and institutions

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

PRC data protection law provides that the state will protect information that is able to identify the identity of individual citizens and information concerning the personal privacy of citizens. The law does not exempt any sector or institution from adherence to the requirements of due process in the performance of their respective offices, and no areas are beyond its scope; provided, however, that a particular aspect of the data protection law may, in some cases, be pre-empted by another law in such areas as national security or policing.

The PI Security Specifications identify certain potential exemptions, pursuant to which data subject consent for the collection and use of PII may not be requisite in the circumstances outlined below:
- circumstances that are directly related to national security or the security of national defence;
- circumstances that are directly related to public security, public health or public interest;
- circumstances that are directly related to the detection of crime or such prosecution, trial or the enforcement of judgment;
- circumstances that involve the protection of life, personal property or other material and legitimate interests of the subject individual or related persons, but where obtaining individual consent is impractical;
- if the PII has already been voluntarily disclosed and made public by the subject individual;
- if the PII is to be collected from public information that has been legally disclosed;
- when necessary for the execution or performance of a contract as requested by the subject individual;
- when necessary for the maintenance of a product or service, eg, to detect and deal with the malfunction of a product or service;
- collection by a news agency for the lawful purpose of reporting; and
- collection by an academic research institution for the purpose of statistics or research, and where such PII has been de-identified prior to its publication.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The interception of communications is governed by the PRC Telecommunication Regulations, which prohibit the unlawful interception of communications of other persons by any person or organisation. Lawful interception is permitted including, for example, required monitoring of any telecommunications network by its operator, which is obligated to terminate the transmission of illegal content, to maintain records and to report incidents to the relevant government authorities.

Electronic marketing is regulated by the PRC Advertisement Law, the Protection of Consumer Rights and Interests Law, and the Administrative Measures on Internet Email Services (the MIIT Email Measures), as well as certain industry-specific regulations, such as CBRC's Measures for the Supervision and Administration of Credit Card Business of Commercial Banks and the CBIRC's Administrative Measures for Telemarketing of Life Insurance.

Unlawful monitoring and surveillance of individuals is governed by the PRC Postal Law, the PRC Criminal Law and the PRC Telecommunication Regulations, among others.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

China's data protection-related legal provisions are distributed among various laws, regulations, implementing measures and other guidance. In addition to certain umbrella laws such as those identified in question 1, industrial sector-specific laws and regulations provide relevant guidance to subject individuals and organisations in numerous discrete areas, including those listed below.
- Banking: for example, the CBRC Circular on the Guidelines for Banking Consumer Protection (effective 30 August 2013); the CBRC Guidelines for Commercial Banks on Management of Information Technology Risks (effective 1 June 2009); the CBRC Guidelines for the Regulation of Information Technology Outsourcing Risks of Banking Financial Institutions (effective 16 February 2013); the PBOC Circular on Doing a Good Job by Banking Financial Institutions in Protecting Personal Financial Information (effective 1 May 2011); and the PBOC Opinion on Further Strengthening the Info Security of Banking Financial Institutions (effective 18 April 2006).
- Consumer Protection: for example, the Protection of Consumer Rights and Interests Law (effective 15 March 2014); the Measures for Punishments against Infringements on Consumer Rights and Interests (effective 15 March 2015); and the Measures on the Administration of Online Trading (effective 15 March 2014).
- Credit Reporting: for example, the Administrative Regulations on the Credit Reporting Industry (effective 15 March 2013); the Circular of the PBOC on Further Intensifying Management of Credit Information Security (effective 2 May 2018); the Administrative Measures for the Basic Databases of Personal Credit

Information (effective 1 October 2005); and the Circular on the Relevant Issues on Regulating Commercial Banks' Obtaining Authorisation to Inquire about Individual Credit Reports (effective 17 November 2005).
- Healthcare: for example, the Prevention and Treatment of Infectious Diseases Law (effective 2 February 1989 and most recently amended 29 June 2013); the Trial Measures for the Administration of Population Health Information (effective 5 May 2014); and the Administrative Provisions on the Medical Records of Medical Institutions (effective 1 January 2014).
- Postal and Courier Services: for example, the Security Measures on the Protection of Users' Personal Information for Mailing and Courier Services (effective 26 March 2014).
- Telecommunications and Internet: for example, the PRC Telecommunication Regulations (effective 25 September 2000, and most recently amended 6 February 2016); the Administrative Measures for the Protection of International Networking Security of Computer Information Networks (effective 30 December 1997); the Interim Provisions on the Administration of the Development of Instant Messaging Services (effective 7 August 2014); the Several Provisions on Regulating the Market Order for Internet Information Services (effective 15 March 2013); the Notice on Strengthening Administration over Network Access by Mobile Intelligent Terminals (effective 1 November 2013); and the Provisions on Protection of Personal Information of Telecommunication and Internet Users (effective 1 September 2013).

Other significant, relevant legal provisions include the Resident Identity Cards Law (effective 28 June 2003, and most recently amended 1 January 2012), the Protection of Minors Law (effective 1 January 2013), and the Administrative Measures for Records of Individual Social Insurance Rights and Interests (effective 1 July 2011).

8 PII formats

What forms of PII are covered by the law?

Generally, PRC laws and regulations apply a functional definition to the identification of PII, often including a non-exclusive listing of examples. For example, in the Interpretation on Several Issues regarding Application of Law in Criminal Cases involving Infringement of Citizen's Personal Information, jointly promulgated by the Supreme People's Court and the Supreme People's Procuratorate, PII is defined as 'information which is recorded electronically or by other means and which, by itself, or together with other information, could be used to identify a citizen or reflect a citizen's movement, including but not limited to a name, identification number, contact information, home address, bank or other account number and password, property details and track of movements'. Early legislation (eg, the 2012 NPC Network Decision) specified 'electronic' media; however, more recent legislation, such as the Cyber Security Law, expressly encompasses any personal data 'kept in electronic form or any other forms'.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

PRC law does not expressly address the potential extraterritorial reach of the law with respect to PII-related matters. In principle, any organisation or individual, including any foreign entity with or without legal presence in China, would be subject to the PRC data protection laws if it collects, processes or uses the PII of PRC citizens within the territory of China, or if they transfer such data into or out of China.

10 Covered uses of PII

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

All processing or use of the PII of PRC citizens is covered under various data protection laws and regulations; however, no distinction is drawn between PII owners and PII processors. Broadly speaking, the law invests each respective citizen with discretionary authority over the distribution and usage of their PII, and obligates each recipient to limit PII use to the scope of permitted usage.

The Data Protection Guidelines and PI Security Specifications provide relevant non-binding, recommended best practices and managerial and technical standards. For example, before a data controller entrusts PII to a third party for processing, it should conduct a security impact assessment to ensure that such data processor has the necessary data security capability. The data processor must strictly abide by the requirements of the data controller on data processing activities and should assist the data controller to fulfil its obligations to the data subject.

Legitimate processing of PII

11 Legitimate processing – grounds

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

Requirements regarding the legitimisation for processing of PII on specific grounds are an established theme in PRC law, and recent legislative developments have reflected an increased emphasis on this topic. Data subject consent as a basis for processing legitimacy was originally established in the 2012 NPC Network Decision. Subsequently, the Protection of Consumer Rights and Interests Law restated and expanded this principle. Most recently, the Cyber Security Law has mandated data subject consent as a prerequisite for cross-border data transfer, and more detailed implementing rules are under development (see 'Update and trends').

In the dimension of criminal culpability, the Interpretation on Several Issues regarding Application of Law in Criminal Cases involving Infringement of Citizen's Personal Information, jointly promulgated by the Supreme People's Court and the Supreme People's Procuratorate, recognises legal obligations as a mitigating factor in assessing culpability for alleged infringement on PII.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

PRC law imposes relatively more stringent processing rules for specific types of PII, including:
- personal financial information;
- personal credit information; and
- personal health information, as further described below.

Personal financial information (PFI)

The PBOC Circular on Doing a Good Job by Banking Financial Institutions in Protecting Personal Financial Information (effective 1 May 2011) provides an expansive definition of PFI, emphasises the statutory obligation of banking financial institutions to protect PFI, and establishes detailed requirements governing its collection, processing and retention. For the purposes of this rule, PFI encompasses:
- personal identity information;
- personal property information;
- personal account information;
- personal credit information;
- personal financial transaction information;
- derivative information, including personal consumption habits, investment willingness and other information that reflects the circumstances of a certain individual and that is formed by processing or analysing the source information; and
- other personal information obtained or stored in the process of establishing business relationships with individuals.

PFI collected within China must be stored, processed and analysed within China. No transfers of domestic PFI overseas are permitted unless otherwise authorised. Any employees with access to PFI must make confidentiality undertakings in writing before assuming such posts. Where a banking financial institution obtains the written authorisation or consent of a client through standard terms, it must also explicitly warn of the possible consequences of such consent in an eye-catching place of the agreement in simple words and remind clients to consider the above warning when such client signs the

agreement. When conducting business through outsourcing, banking financial institutions must assess the ability of outsourcing service suppliers in protecting PFI, and treat such ability as an important indicator for choosing outsourcing service suppliers. In the event of a data breach involving PFI, the relevant banking financial institution must report relevant information as well as preliminary disposal opinion to the local branch of the PBOC within seven working days of the occurrence of discovery.

Personal credit information (PCI)

The Administrative Regulations on the Credit Reporting Industry (effective 15 March 2013) provide detailed guidance with respect to credit information, particularly with respect to adverse personal information that may have a negative impact on the credit status of the individual or entity, for example, information concerning a failure to perform contractual obligations in such activities as borrowing; purchases on credit; guarantees; leasing; insurance; using credit cards; information on administrative punishments; information on court judgments; rulings requiring the individual or entity to perform his, her or its obligations; and information on enforcement and other adverse information specified by the relevant authorities.

Without a data subject's consent, no PCI may be collected by a credit reporting entity other than such information as is required to be disclosed in accordance with the law. Additionally, any information provider intending to provide a credit reporting entity with any adverse information on any individual must first notify the individual, with the exception of information that is required to be disclosed in accordance with the law. Credit reporting entities are expressly prohibited from collecting personal information in relation to religion, genes, fingerprints, blood type, disease and medical history and other information that is prohibited by law.

The assembly, storage and processing of information collected by a credit reporting entity from within the territory of China must also be carried out within the territory of China. A credit reporting entity may not retain adverse information for more than five years after the date when the corresponding misconduct or adverse event ended, and during this period it must maintain records on any explanation provided by the data subject for such adverse information.

Throughout the storage term, each credit reporting entity must maintain a record of its employees' access to such individual credit information, including the names of employees who have accessed such information, the time when they accessed such information, the information they accessed, and the purposes for which they accessed such information.

An individual or entity concerned may apply to a credit reporting entity to access information on themselves. Where an individual or entity deems that there is any error or omission in the information, the individual or entity is entitled to raise an objection and require necessary corrections. An application to a credit reporting entity for access to information on an individual must be subject to the written consent of the individual and agreement between the applicant and individual specifying the purposes for which such information may be used, with the exception of information that may be accessed without the consent of the individual in accordance with law.

Personal health information (PHI)

The Trial Measures for the Administration of Population Health Information emphasise the statutory obligation of PRC health and family planning authorities and service institutions to protect population health information, including PHI, and establishes detailed requirements governing collection, processing and retention. For the purposes of these measures, PHI means the health information, medical records and other related information arising from the lawful process of PRC health and family planning services and management. PHI may not be stored in overseas servers (including servers hosted in and leased from foreign countries).

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Subsequent to lawful collection, and in the absence of a change with respect to the consented treatment of PII, PRC law does not establish any general obligation to provide notice to or consult with a data subject with respect to collected PII.

The Data Protection Guidelines propose that a consent notice to a prospective data subject should encompass identification of the following:

- the purpose and method of collection;
- the detailed content of collection;
- the retention period;
- the scope of use;
- security measures;
- the data administrator's contact details;
- the potential risks and consequences if the PII is or is not provided;
- the complaint procedures; and
- anticipated transfers to third parties.

Standards for the evaluation of issues such as change in consented purpose, content, retention period, scope of use, security or other matters have not received meaningful attention with respect to legislation, litigation or judicial interpretation in China. Accordingly, in the absence of specific contractual provisions, the relevant threshold for a notification obligation would be uncertain. However, draft regulations have been proposed that, if implemented, would require any third party to ensure that relevant consent has been lawfully obtained prior to any overseas data transfer, and would preclude such transfer unless proper consent had been obtained (see 'Update and trends').

14 Exemption from notification

When is notice not required?

Subsequent to lawful collection, and in the absence of a change with respect to the consented treatment of the PII, PRC law does not establish a general obligation to provide notice to or consult with a data subject with respect to collected PII.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The Cyber Security Law provides a data subject with the right to request any network operator to correct mistakes in any collected PII, as well as a right to request the deletion of PII in the event of a network operator gathering or using such PII in violation of the provisions of laws and regulations or the agreements between the data subject and network operator.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The Data Protection Guidelines establish a principle of quality assurance, which requires that the data administrator must ensure that any PII being processed is confidential, complete, available and up to date. Consonant with this principle, specific rules, including the Cyber Security Law, permit any data subject to inspect and correct or clarify recorded PII in certain circumstances.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

In principle, PRC law restricts the collection and use of PII to that which is lawful, legitimate and necessary. With limited exceptions, PRC law does not expressly restrict either the amount of PII that may be held or the length of time it may be held. One exception to this general

approach is the credit reporting industry, which mandates that a credit reporting entity may not retain adverse information for more than five years after the date when the corresponding misconduct or adverse event ended (see question 12).

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The 'finality principle' has not been adopted in the PRC. There is no express limit on the purposes for which PII may be used, except that such uses must be lawful, legitimate and necessary, and must conform to the purpose notified to and consented by the data subject.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Unless otherwise permitted by law, any new use of PII for a purpose beyond the scope which has been consented by the data subject is prohibited, unless the data subject provides their consent to such new purpose. Standards for the evaluation of issues such as change in consented purpose and scope of use have not received meaningful attention with respect to legislation, litigation or judicial interpretation in China. Accordingly, in the absence of specific contractual provisions, the relevant threshold for a determination of the establishment of a new purpose would be uncertain.

Security

20 Security obligations

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

Overarching legislation such as the 2012 NPC Network Decision and the Protection of Consumer Rights and Interests Law establishes a general requirement that enterprises and public institutions must employ both technical and other necessary measures to ensure information security, and to prevent the PII of PRC citizens collected during business activities from being leaked, damaged or lost. The Cyber Security Law materially strengthens PII protection protocols by establishing a robust security assessment apparatus as a prerequisite for cross-border data transfers.

More detailed direction has been promulgated by competent authorities and industry regulators directing the development and adoption of managerial and technical precautions to prevent the loss, destruction or disclosure of protected information. For example, the Provisions on Protection of Personal Information of Telecommunication and Internet Users, providing detailed guidance, require that telecommunication operators and internet information services providers must, as a minimum, implement the below-listed discrete technical, organisational and other security measures in order to protect users' PII:

- determine the PII security management responsibilities of each department, position and branch;
- establish a workflow and security management system for the collection, use and other relevant PII-related activities;
- carry out access management over personnel and agents;
- carry out examinations on the export, reproduction or destruction of information in batch, and implement relevant anti-leakage measures;
- properly store printed, optical and electronic media and other systems for recording PII, and implement corresponding safe storage measures;
- carry out connection examinations for the information system storing PII, and implement relevant anti-hacking and anti-virus measures;
- record the person, time, place, event and other information in connection with any conduct carried out with respect to PII;
- carry out telecommunication network security prevention work pursuant to the requirements of telecommunication authorities; and
- other necessary measures as provided by the telecommunication authorities.

21 Notification of data breach

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?

Overarching legislation such as the 2012 NPC Network Decision and the Protection of Consumer Rights and Interests Law requires that, if it is determined that PII may have been or is leaked, damaged or lost, then responsible enterprises and public institutions are obligated to immediately institute remedial measures. This general approach is repeated in many industry-specific directives, with increasing degrees of specificity. In terms of reporting obligations, some regulations (eg, the Provisions on Protection of Personal Information of Telecommunication and Internet Users) mandate timely notification to the responsible governmental authority. Most recently, the Cyber Security Law mandates that notification be provided to the data subjects in accordance with regulations, without providing further detail.

The PI Security Specifications recommend that, when a security incident occurs, the data controller should notify the affected individual by means of email, letter, telephone call or online post. If it is difficult to notify each data subject, a data controller may consider employing a public warning.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

There is no PRC law or rule of general applicability that mandates the appointment of a data protection officer. But such a requirement, separate and distinct from IT appointments, has been established or proposed in certain guidelines, industry-specific regulations or draft regulations. Examples include the PI Security Specifications, the CBIRC's Guidelines for the Regulation of the Information System Security of Insurance Companies (for Trial Implementation) and the Trial Measures for the Administration of Population Health Information.

The PI Security Specifications recommend that data controllers appoint a responsible person and establish an internal function for PII protection. If a data controller meets any of the following conditions, a dedicated department must be established and a responsible person appointed to undertake PII protection responsibilities: its main business involves processing PII and it has more than 200 staff who engage in such business; or it processes the PII of more than 500,000 individuals, or projects that it will process the PII of more than 500,000 individuals within 12 months.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The requirement to maintain internal records and establish internal processes and documentation is established in industry-specific regulations, and particularly emphasised in such areas as banking and finance, credit reporting, health and telecommunications.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The PI Security Specifications recommend that data controllers conduct an annual personal information security impact assessment in order to periodically evaluate compliance with relevant data security principles, and the impact of the processing activities on the data subjects. In addition, an ad hoc security impact assessment is recommended whenever there is a change in data protection laws, or a material change occurs in the enterprise's business model, IT system or operational environment, or upon the occurrence of a security incident.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

PII owner and PII processor registration with a supervisory authority is not mandated by any generally applicable or industry-specific PRC law or regulation.

26 Formalities

What are the formalities for registration?

See question 25.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

See question 25.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

See question 25.

29 Public access

Is the register publicly available? How can it be accessed?

See question 25.

30 Effect of registration

Does an entry on the register have any specific legal effect?

See question 25.

31 Other transparency duties

Are there any other public transparency duties?

There is no PRC law or rule of general applicability that mandates an organisation to make public statements as to the collection, use or processing of PII.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

No PRC law generally governs PII transfer in the context of outsourced processing services. However, the Cyber Security Law requires that any transfer of PII to third parties is subject to consent by the data subject and, if the outsourcing involves an outbound, cross-border PII transfer, then specific security assessment procedures will apply (see question 34).

Generally, circumstances surrounding the transfer of PII to entities that provide outsourced processing services may vary considerably, depending on the industry and enterprise business model. Industrial regulators (eg, those regulating the banking and finance, public health and insurance industrial sectors) may provide general and specific relevant guidance including, for example, outsourcing of sensitive functionality.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Other than general requirements as to notice, choice or purpose limitation, and data subject consent, restrictions with respect to disclosure of PII to other recipients are not described in any generally applicable PRC law. Industrial regulators may supplement guidance governing regulated individuals and organisations. Unconsented disclosure of PII to a third party is punishable by criminal and administrative penalties pursuant to applicable law.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The cross-border transfer of PII is generally regulated by the Cyber Security Law, as supplemented by relevant industry-specific regulations. Recently promulgated and effective from 1 June 2017, the Cyber Security Law, among other things, establishes a framework aimed at safeguarding PRC citizens' PII and other important information with respect to cross-border transfers. The precise significance of some provisions is unclear, and specific application may vary dependent on the final form of implementing measures to be published separately (see 'Update and trends').

The Cyber Security Law's PII protection framework includes three principle components: data localisation, consent and pre-transfer security assessment.

- Data localisation: business necessity as a pre-requisite for transfer. As a general rule, if PRC citizens' PII is not required to be transferred overseas, then it should not be transferred.
- Data subject consent: cross-border transfer of PRC citizens' PII without prior data subject consent is strictly prohibited.
- Pre-transfer security assessment: prior to a PII cross-border transfer, the transferor must complete a security assessment that demonstrates a satisfactory cross-border transfer. In many circumstances, an organisation may complete a self-assessment; however, in the case of large-scale PII transfer operations, the assessment must be accomplished by the competent governmental authority.

In addition to the Cyber Security Law, industry-specific examples of cross-border regulation include the PBOC's Circular on Doing a Good Job by Banking Financial Institutions in Protecting Personal Financial Information and the Trial Measures for the Administration of Population Health Information, prohibiting cross-border transfers of personal financial information or personal health information.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

See question 34.

36 Further transfer

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

The Cyber Security Law contemplates that PRC citizens' PII transfers outside of the PRC may be subject to restriction or authorisation. The precise requirements are as yet unclear, and will be dependent on the final form of implementing measures to be published separately (see 'Update and trends').

Rights of individuals

37 Access

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

The Data Protection Guidelines state that PII owners should provide data subjects with PII access routinely and free of charge, unless the cost of informing or frequency of request is beyond a reasonable range. This principle has not been reiterated in any PRC law of general applicability, although the credit reporting industry has incorporated responsive provisions in relevant regulations. In the credit reporting industry, a data subject has the right to make an inquiry with the credit reporting agency about their personal information, and has the right to be provided with a credit report from the credit reporting agency twice a year, free of charge (see question 12).

Update and trends

In the past year, China has witnessed important regulatory developments relating to data protection, including publication of:

- the China Cyber Security Law;
- the Information Security Technology – Personal Information Security Specifications (GB/T 3527302017), (the PI Security Specifications);
- the draft Measures for Evaluating the Security of Transmitting Personal Information and Important Data Overseas (Draft PI Transfer Measures);
- the draft Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft Data Transfer Guidelines); and
- the draft Regulations on Cybersecurity Multi-level Protection Scheme (Draft Multi-Level Protection Scheme).

China Cyber Security Law

The Cyber Security Law was promulgated in November 2016, with effectiveness from 1 June 2017, and establishes an overarching cybersecurity framework. Within that framework, supporting measures to provide relatively more detailed implementation guidance are under development, as further described below. Other relevant rules are expected to be forthcoming, as China's regulatory authorities proceed with concrete steps towards implementing the overarching protective framework codified in the Cyber Security Law. Certain aspects of these new laws and regulations are unclear, and subject to further clarification by relevant authorities. But the evident trend of regulation will increase the compliance burden of companies, notably with respect to cross-border data transfers and data localisation.

PI Security Specifications

The PI Security Specifications were promulgated on 29 December 2017, with effectiveness from 1 May 2018. Among other features, the PI Security Specifications define 'personal information' and 'sensitive PI', and provide a list of PI and sensitive PI examples and identification guidance. The PI Security Specifications set out 'consent' requirements for direct and indirect collection of PII and, for the first time, provide exceptions to the consent requirement (see question 5). The PI Security Specifications recommend the implementation of security audit procedures, including automated procedures, in order to evaluate effectiveness and to monitor and record the PI processing procedures. A standard form of privacy policy is also introduced. Although the PI Security Specifications are non-mandatory, in practice, it may be relied upon by PRC governmental authority when evaluating the preparedness and performance of a PII controller or related party. For example, in January 2018, CAC officials issued an oral warning to a Chinese online payment company that its use of a default tickbox to automatically obtain a user's consent to its updated privacy policy was in violation of the PI Security Specifications.

Draft PI Transfer Measures

The Draft PI Transfer Measures propose detailed guidance with respect to the implementation of a security assessment programme, featuring network operator self-assessments and by data export plans, setting out the purpose, scope, type and scale of the data export, the IT system involved, the transit country and the destination, and the security control measures to be taken. The security assessment is required to prove the proposed outbound transfer is lawful and justified, and that the risks are controllable. The degree of risk involved with each transfer will be assessed by taking into account the characteristics of the data (eg, the volume, scope, type, sensitivity and technical measures), and the possibility of security breach incidents, which requires an evaluation of the technical safeguards and management capabilities of both the data exporter and the recipient, as well as the legal and political environment of the destination country.

Draft Data Transfer Guidelines

The Draft Data Transfer Guidelines are principally concerned with ordering a system for assessing the security of cross-border data transfers, including the establishment of a two-tier assessment framework, comprising network operator self-assessments and, where required, governmental assessments. A network operator self-assessment would include pre-transmission assessments and periodic assessments to be conducted at least annually. Of particular significance, the Data Transfer Guidelines, for the first time, propose a specific framework to guide the conduct of mandated security assessments, expanded to encompass every 'network operator' and, by reference, any other person or entity involved with the provision of regulated data to an overseas destination.

Draft Multi-Level Protection Scheme

The Multi-Level Protection Scheme proposes detailed measures to support implementation of any multi-level protection scheme established by a network operator pursuant to the requirements of the China Cyber Security Law.

38 Other rights

Do individuals have other substantive rights?

The Data Protection Guidelines provide that PII owners should be invested with certain substantive rights, including the right to correct inaccuracies, but does not address the specific topic of data subject control over particular kinds of processing, except to the extent of being informed about the intended uses and being accorded a right to withhold consent. The right to correct inaccuracies has been affirmed in certain industrial contexts, including credit reporting, and most recently included in the new Cyber Security Law, which also provides that, if an individual should discover that a network operator has collected or used their PII in violation of the provisions of laws and regulations or their agreements, they have the right to request that the network operator delete any PII.

39 Compensation

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?

Pursuant to the Tort Liability Law, an individual or entity that breaches the law and infringes on or harms a PRC citizen's PII may assume tortious liability. Under such circumstances, in addition to certain other remedies (eg, cessation of the infringement, apology), a tortfeasor may be subject to payment of monetary damages or compensation. For example, a tortfeasor could be required to pay reasonable costs for medical treatment. However, compensation normally will not be awarded unless losses are actually incurred. In theory, the law also recognises serious mental suffering arising from PII damage or infringement as a basis for compensation. However, in practice, the courts have adopted a conservative approach in such determination, and compensation for mental damages has rarely, if ever, been granted.

40 Enforcement

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

An individual or organisation may file a complaint to the relevant supervisory authority, which may order regulated individuals and organisations to fulfil their obligations to protect personal information. Such authorities typically have a variety of administrative sanctions at their disposal to encourage cooperation, including private and public warnings, fines and, in serious cases, control over licensing and the power to refer a matter for criminal prosecution. However, in order to obtain monetary compensation or a judicial order to enforce rights in PII, an aggrieved individual or organisation must avail themselves of the PRC court system.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

PRC law does not include any additional general derogations, exclusions or limitations.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

PII owners who are unsatisfied by the orders of a supervisory authority may bring a lawsuit against such supervisory authority before a court. The PRC Administrative Litigation Law and the Interpretations on Several Issues concerning the Implementation of the Administrative Litigation Law promulgated by the Supreme People's Court provide more detailed guidelines regarding the procedures for the judicial review of administrative orders.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Requirements or standards with respect to the use of cookies has not received meaningful attention with respect to legislation, litigation or judicial interpretation in China. Accordingly, use of cookies would not be prohibited if users were provided notice of the cookies' usage, and if the particular application does not otherwise violate PRC legal requirements, for example, by collecting PII.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Electronic communications marketing is generally regulated by nationwide legislation such as the Protection of Consumer Rights and Interests Law and the MIIT Email Measures. Relevant industry regulators such as the CBIRC have also furnished sector-specific regulation. Pursuant to these laws and regulations, the transmission of unsolicited marketing communications is generally prohibited. For example, pursuant to the Protection of Consumer Rights and Interests Law, a company is prohibited from transmitting commercial information to the individuals without consent. The Email Measures specify more detailed requirements providing, for example, that:

- no organisation or individual may send an email containing commercial advertisements without the express consent of the recipient;
- any organisation or individual that does send emails containing commercial advertisement content must mark them with the word 'advertisement' or 'AD' at the beginning of the email title;
- emails containing commercial advertisements must provide contact information to the receiver to enable them to refuse receipt of further emails; and
- where an email recipient first agrees to receive emails containing commercial advertisement content, but later withdraws such consent, then the email sender must cease sending such emails unless otherwise agreed.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Requirements or standards with respect to the use of cloud computing services have not yet received extensive attention with respect to legislation, litigation or judicial interpretation in China. PRC laws that emphasise data localisation may impinge on the use of cloud computing services where they impose limitations on cross-border transfer, potentially encouraging technical protective measures such as anonymisation or encryption, and limiting or restricting storage of certain forms of PII to domestic cloud servers physically located within the geographical limits of China.

Recently, the MIIT issued the draft Notice on Regulating the Business Activities in the Cloud Computing Service Market (published 24 November 2016), which proposes that cloud computing service providers must adopt certain specific measures for the protection of network data and PII, including:

- to establish and publicise rules on the collection and use of PII;
- to adopt security safeguard measures against theft, and ensure data backup;
- to cease the collection and use of PII whenever a user terminates their service;
- for services targeted at domestic customers, the servers and data must be stored within China and cross-border transfer of data shall comply with relevant regulations; and
- in case of a data leakage, provide customers with timely notification, take effective remedial actions and report to the telecommunications regulator.

JINCHENG TONGDA & NEAL
金诚同达律师事务所

Vincent Zhang **vincentzhang@jtnfa.com**
John Bolin **johnbolin@jtnfa.com**

10th Floor, China World Tower A
No. 1 Jianguo Menwai Avenue
Beijing
China

Tel: +86 10 5706 8585
Fax: +86 10 8515 0267
www.jtnfa.com

Colombia

María Claudia Martínez Beltrán
DLA Piper Martínez Beltrán Abogados

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The Colombian Constitution defines in articles 15 and 20 two fundamental rights regarding PII: data protection or habeas data and proper rectification upon mistakes. Moreover, two statutory laws and several decrees have regulated PII protection and the obligations derived from the processing of personal data.

Statutory Law 1266 of 2008 states various general terms on habeas data and specifically regulates the protection and processing of data contained in credit bureaux, financial entities, credit records, commercial information and any information obtained from abroad. Indeed, this law establishes basic principles for data treatment, the rights of data subjects, the duties of PII owners, and some specific rules for financial data.

Statutory Law 1581 of 2012 specifically regulates PII protection and processing along with databases, and is the general framework for data protection in Colombia. In this regard, it defines special categories of PII such as sensitive data and data from children and teenagers. Moreover, it regulates the authorisation and procedures for data processing and creates the National Register of Databases. Indeed, except for the matters regulated under Law 1266 for the financial sector, Law 1581 pf 2002 is applicable for all other industries.

Decree 1377 of 2013 is a piece of secondary regulation that outlines the way in which personal and domestic databases should be treated, complementing what is stated in Law 1581 on the authorisation of personal data usage and recollection, limitations to data processing, cross-border transfer of databases and privacy warnings, among others.

Finally, Decree 090 of 2018, issued by the Ministry of Commerce, Industry and Tourism, regulates the National Register of Databases.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

According to Law 1266, there are two different authorities on data protection matters. The first, which acts as a general and main authority, is the Superintendence of Industry and Commerce (SIC). The second authority is the Superintendence of Finance (SFC), which acts as a supervisor for financial institutions, credit bureaux and other entities that manage financial or credit records regarding what is stated in Law 1266.

Nevertheless, under Law 1581, the SIC is the maximum authority in personal data protection. For this reason, it is empowered to investigate, sanction, block the treatment of personal data as an injunctive relief, promote data owners' rights, give policy directions, require any type of information from companies and carry out inspections.

3 Legal obligations of data protection authority

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

The SIC oversees that PII owners and data processors comply with their obligations on data protection. For this reason, among others, the SIC is empowered to request the cooperation of international or foreign authorities when the rights of data subjects are infringed abroad (eg, by the international collection of PII).

4 Breaches of data protection

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

The SIC is an administrative authority that may sanction businesses, companies or in general any entity with fines up to 2,000 times the Colombian minimum legal wage, order instructions to comply with the data protection regime or order the temporary or permanent foreclosure of the company, entity or business.

Moreover, the Colombian Criminal Code contemplates personal data violation as a criminal penalty in the following terms: anyone who, without authorisation, seeking personal or third-party gain, obtains, compiles, subtracts, offers, sells, interchanges, sends, purchases, intercepts, divulges, modifies or employs personal codes or data contained in databases or similar platforms, will be sanctioned with 48 to 96 months in prison, and a fine from 100 to 1,000 times the Colombian minimum legal wage. These sanctions will also apply to those individuals who design, develop, traffic, sell, execute or program websites, links or pop-up windows with an illicit purpose and without authorisation. In Colombia companies are not subject to criminal penalties, and therefore the employees or managers can be criminalised for this.

Finally, since privacy and the correct maintenance of personal data are fundamental constitutional rights in Colombia, citizens are entitled to pursue protection before any Colombian judge via a special constitutional action. Any judge could order a private or public entity to modify, rectify, secure or delete personal data if it is kept by means that violate constitutional rights. Constitutional actions can take up to 10 days to be resolved and the failure to comply with an order may result in the imprisonment of the legal representative or the person responsible for the violating entity.

Scope

5 Exempt sectors and institutions

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

The exempt sectors and institutions outside the scope of the Colombia data protection regime are:

- databases included in Law 1266, as set forth in question 1;
- personal or domestic databases: PII treated for personal or domestic purposes shall not comply with the obligations set forth in the Colombian Regime on Personal Data. However, the prior authorisation of the data subject is required when such PII is going to be

disclosed to third parties that are going to treat the data for commercial purposes;
- databases aiming to protect and guarantee national security, prevent money laundering and the financing of terrorism: the PII regarding national security shall be treated according to the principles and regulations regarding intelligence and national security. Moreover, the personal data referred to the prevention of money laundering and the financing of terrorism shall comply with the provisions in Law 529 of 2006;
- databases of the intelligence and counterintelligence agencies: when the information is being processed by an intelligence or counterintelligence agency, the authorisation of the data subject is not required. Nevertheless, if within the investigation the data processor finds relevant information for criminal law purposes, it shall send it immediately to the corresponding judicial authorities so it can be used as legal proof and the rights and guarantees of the data subject are not violated;
- news and media databases: this kind of PII is governed by Law 51 of 1975 since it relates to freedom of expression; and
- databases regulated by Law 79 of 1993 (on population census): as per article 5 of said law, individuals and legal entities that are domiciled or reside in Colombia shall provide to the National Statistics Administrative Department data requested within censuses and surveys.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Data Protection Regime is applicable to any type of communication that is delivered to individuals. However, the content of communications is covered by the consumer protection regime.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

PII in Colombia is governed by Law 1581 of 2012, except for the databases set forth in the question regarding sectors and institutions above.

However, it is important to bear in mind that not all PII is processed in the same manner, since Law 1581 of 2012 brings special categories of PII, such as:
- sensitive PII: data that affects its data subject's intimacy or the erroneous usage of which might cause discrimination (eg, ethnic or racial origin, political orientation, religious or philosophical convictions, membership of a labour union, human rights group or social group, membership of a group that promotes any political interest or that guarantee rights of political parties from opposing groups, health, sexual conviction and biometrics); and
- PII of children up to 18 years old.

8 PII formats

What forms of PII are covered by the law?

The Colombian Regime on Data Privacy applies to all PII in Colombia, including electronic and physical records or databases, which have to have a security policy depending if it is one or another.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Law 1581 applies to all owners and processors that treat data in Colombia, and to those data controllers or data processors obliged to apply the Colombian law as per international treaties.

10 Covered uses of PII

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

The Colombian Regime on Data Privacy distinguishes between who controls or owns the PII (the PII owner) and who provides PII processing services (the data processor). Moreover, when processing PII, PII owners and data processors shall guarantee that PII is kept within strict security measures and that it is not modified without prior authorisation from the data subject. For this reason, PII owners and data processors shall comply with any and all of the obligations set forth in Colombian legislation for PII processing, which are similar but have minor differentiations.

PII owner obligations

A PII owner shall:
- guarantee that data subjects are able to effectively exercise their right to habeas data;
- request and store a copy of authorisations granted by data subjects;
- inform data owners about the purpose for which the data is collected and processed;
- guarantee data security conditions;
- guarantee that the information supplied is accurate, truthful, complete, updated, verifiable and understandable;
- update the information and promptly communicate any changes to the data processor;
- rectify the information when it is not correct;
- only transmit to the data processor the personal data authorised by the data subject;
- require the data processor to have optimal security conditions;
- process the data subject's requests and complaints;
- adopt a data privacy policy;
- inform the data processor when any data subject's data is under complaint;
- inform any data breach to the SIC; and
- comply with any SIC requirements.

Data processor obligations

A data processor shall:
- guarantee that data subjects are able to effectively exercise their right to habeas data;
- store data in a safe and secure environment;
- update data provided by the PII owner in a five-day period after the notice is received;
- respond to any inquiries and complaints raised by data subjects;
- adopt a data privacy policy;
- not circulate data that has been disputed by the data subject or the SIC;
- permit data access only to people that are subject to access the data;
- inform data breaches to the SIC; and
- comply with the instructions given by the SIC.

Legitimate processing of PII

11 Legitimate processing – grounds

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

The PII owner and data processor shall always have the authorisation of the data subject in order to carry out PII treatment. Under Decree 1377, consent may be obtained in writing, orally or by the owner's unequivocal behaviour demonstrating that consent and authorisation have been given (under Colombian law, silence or tacit consent is not valid and thus cannot be interpreted as unequivocal behaviour). Also, Decree 1377 requires PII owners to retain proof of the data subject's consent.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Sensitive PII may only be processed:
- with a special and specific authorisation given by the data subject;
- when it is necessary to preserve the owner's life or a vital interest;
- when the data is related to the members of an NGO or association;
- when it is related to or fundamental for the exercise of a judicial right; or
- when the data has an historic, statistical or scientific means, in which case the identity of the owner must not be disclosed.

To obtain the consent for sensitive PII processing, the PII owner shall expressly inform the owner that since the data is sensitive, it is not compelled to authorise the treatment of such data; and, prior to collection, inform the data subject of the specific purposes for the processing of each category of sensitive data, obtaining specific consent to such.

The processing of PII of children is forbidden in Colombia, unless the PPI processed is considered public information or the legal guardian's consent is obtained to process the data. In all cases, the rights of children shall always prevail.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Data controllers must notify individuals that they hold their PII if the data subject demands such information. Therefore, this information does not have to be automatically notified to the data subject.

14 Exemption from notification

When is notice not required?

Not applicable.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The data subject will always be the owner of the PII it provides to the PII owner. For this reason, the data subject has the right to:
- be informed of the current uses of the PII;
- submit complaints to the Superintendence of Industry and Commerce regarding violations of the provisions of Law 1581 of 2012, once the process of inquiry or complaint against the PII owner has been exhausted; and
- revoke authorisation to the processing of the personal data and request the removal of such data at any time and for any reason.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

As set forth in question 9, PII owners shall guarantee that the information supplied by the data subject is accurate, truthful, complete, updated, verifiable and understandable. In this regard, the data subject has the right to access, update, rectify and delete his or her personal data at any time, through the mechanisms determined by the PII owner following the legal process established for this purpose. The treatment of partial, incomplete, fractional or error-inducing data is forbidden.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Colombian law sets a limit on the period during which personal data may be processed: data may only be processed for as long as necessary to accomplish the purposes authorised by the data subject. Once those purposes are fulfilled, or in the event that they disappear, the PII owner should stop processing the data. The law does permit further retention of personal data when it is necessary for compliance with legal or contractual obligations.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Personal data is also subject to the principles of restricted purpose and restricted circulation. This means that the scope of the use of information is limited to the purpose for which the information was revealed or supplied and authorised in the first place by the data subject.

Under Law 1581, for the authorisation to be valid it shall be done prior to the data processing and shall be informed, meaning that the data subject shall be aware of the exact purposes for which it has been processed. Indeed, Decree 1377 explains that:
- personal data should be collected and processed in accordance with the purposes authorised by the data subject; and
- such authorisation may be obtained by any means, provided that it allows subsequent consultation.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The data subject shall authorise any new purpose that will be introduced in the processing of the PII. Therefore, the data may be used or treated for new purposes as long as the data controller obtains the authorisation of the data subject.

Security

20 Security obligations

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

PII owners have a legal duty to guarantee that the information under their control is kept using strict safety and security measures. For this reason, they must ensure that such information will not be manipulated or modified without the authorisation of the data subject. Thus, PII owners and data processors shall have proof of evidence of the implementation of appropriate security measures through an information security policy, in which they ensure:
- the existence of administrative and technical safeguards that are proportional to the structure and size of the data controller's business;
- the adoption of internal mechanisms to implement data protection policies, including training and educational programmes; and
- the adoption of procedures for addressing and responding to inquiries, requests and complaints from data owners.

However, encryption is not expressly required.

21 Notification of data breach

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 articles 17(n) and 18(k) of Law 1581, the PII owner and the data processor shall notify the SIC if there is a breach of security codes, a security risk or a risk through data administration. A security risk is defined as the infringement of security codes or the loss, robbery or unauthorised access of information from a database managed by the PII owner or data processor. Therefore, a security incident is considered as any event on manual or systematised databases that threatens the security of the personal data stored therein.

The notification shall include:
- the type of incident;
- the date of the incident;
- the date of knowledge of the incident;

- the cause;
- the type of information compromised; and
- the number of affected owners.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Every PII owner and data processor shall appoint a data protection officer, who will be in charge of responding to and processing queries from data subjects. In addition, the data protection officer shall implement the policies and procedures for complying with the legal regime on data privacy, along with good practices for managing PII, which shall include a programme for data protection and evaluation systems.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The PII owner and data processor shall prove the authorisation granted by the data subject for the PII processing. For this reason, both the PII owner and data processor shall keep a record of the authorisation granted by the data subject as long as the PII treatment is carried out.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Not applicable.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

Databases containing PII where automated or manual processing is carried out by a natural or legal person, in Colombian territory or abroad, will be subject to registration in the National Register of Databases when:

- a company's total assets are greater than 100,000 Tax Value Units (TVUs; 3,315,200,000 Colombian pesos in 2018);
- a non-profit organisation's total assets are greater than 100,000 TVUs (3,315,200,000 Colombian pesos in 2018); or
- the company or entity has a public nature.

26 Formalities

What are the formalities for registration?

The data controller shall register each of database that is processed independently. In addition, each registry requires the following information:

- the identification details of the data controller: business name, tax identification number, location and contact information;
- the identification details of the data processor: business name, tax identification number, location and contact information;
- channels to grant the data subject's rights;
- the name and purpose of the database;
- the form of processing data (manual or automatised);
- security standards; and
- a privacy policy.

Moreover, Decree 090 of 2018 has established the following terms for registering databases:

- data controllers whose total assets are over 610,000 TVUs (approximately US$6,740,000) shall register their databases before 30 September 2018;
- data controllers whose total assets are between 100,000 and 610,000 TVUs (approximately US$1,105,00–6,740,000) shall register their databases before 30 November 2018; and
- data controllers who have a public nature shall register their databases before 31 January 2019.

Any database created after these dates must be registered within two months of its creation.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

The SIC may initiate actions against private entities and sanction them with fines of up to 2,000 times the Colombian minimum legal wage, and the temporary or permanent foreclosure of the company, entity or business.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

The National Register of Databases is a public register and may be accessed online at https://rnbd.sic.gov.co/sisi/consultaTitulares/consultas.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Every PII owner and data processor shall comply with the obligations on data privacy. The registration of databases benefits data subjects, who may consult the principal information regarding PII processing; and the SIC, since it is one of the principal tools to exercise its supervisory functions.

31 Other transparency duties

Are there any other public transparency duties?

Not applicable.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The Colombian Regime on Data Privacy distinguishes between the transfer and transmission of PII.

The transmission of PII takes place when the PII processing implies the communication of data by the PII owner to the data processor, in Colombia or abroad, where the data processor processes personal data on behalf of the PII owner. To transmit PII, the PII owner requires the authorisation of the data subject, or the execution of a transfer agreement with the data processor. In this latter case, the agreement shall include the following clauses:

- the extent and limitations of the data treatment;
- the activities that the data processor will perform on behalf of the PII owner; and
- the obligations the data processor has with the data subject and the PII owner.

Data processors have three additional obligations when processing PII:

- to process data according to the legal principles established in Colombian law;
- to guarantee the safety and security of the databases; and
- to maintain strict confidentiality of the personal data.

The PPI owner that transmits data to a data processor shall identify the data processor in the National Register of Databases. Finally, the data processor shall treat PII in accordance with the PII owner's privacy policy and the authorisation given by the data subject.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

In order to disclose PII, the PII owner or the data processor requires the prior authorisation of the data subject. Nevertheless, the data controller or the data processor do not require such authorisation when:

- the information is demanded by a public or administrative entity by means of a judicial order or exercising its legal duties;
- it is public data;
- a medical or sanitary urgency demands the personal data processing;
- the data processing is authorised by law for historical, statistic or scientific purposes; or
- the data is related to people's birth certificates.

Regarding credit information, the information may only be disclosed to:

- the data subject or third parties authorised by him or her, within the consultation procedure established by law;
- the users of the data (the person or entity that accesses the database and uses the information that has been gathered);
- any judicial or jurisdictional authority upon request;
- any control or administrative authority, when an investigation is ongoing; or
- data processors, whether with the data subject's authorisation, or when no authorisation is needed and the database aims for the same objective or involves an activity that may cover the purpose of the disclosing data processor.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

As per Law 1581, the transfer of personal data occurs when a PII owner located in Colombia sends the personal data to a recipient, in Colombia or abroad, who is responsible for the personal data, becoming a PII owner.

Cross-border data transfer is prohibited unless the country to which the data will be transferred meets at least the same data privacy and protection standards as the ones provided under Colombian regulations. In this regard, adequate levels of data protection will be determined in accordance with the standards set by the SIC.

Authorised countries for the international transfer of personal data are Austria, Belgium, Bulgaria, Costa Rica, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, the Republic of Korea, Latvia, Lithuania, Luxembourg, Malta, Mexico, the Netherlands, Norway, Peru, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, the United Kingdom and the USA.

This prohibition does not apply in the following cases:

- when the data subject has expressly consented to the cross-border transfer of data;
- the exchange of medical data;
- bank or stock transfers;
- transfers agreed under international treaties to which the Colombia is a party;
- transfers necessary for the performance of a contract between the data subject and the controller, or for the implementation of pre-contractual measures, provided the data subject consented; or
- transfers legally required in order to safeguard the public interest.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Yes, a cross-border transfer requires a special authorisation from the SIC when the country to which the PII is going to be transferred does not meet the same data privacy and protection standards as the ones provided under Colombian regulations and that have already been accepted by the authority.

36 Further transfer

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

Yes, but it is important to distinguish if it is under a transfer or transmission scenario.

Rights of individuals

37 Access

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

Yes, data subjects have the right to access to their PII. For this purpose, the PII owner and data processor shall establish simple and agile mechanisms that are permanently available to data subjects so that they can access their personal data and exercise their rights. PII owners must comply with the legal procedure established by law for this purpose, which demands a maximum of days to answer the data subject's request.

Data subjects may consult their personal data free of charge at least once each month, and whenever there are substantial modifications to the privacy policy.

38 Other rights

Do individuals have other substantive rights?

Data subjects have the right to:

- know, update and rectify their PII with the PII owner;
- request evidence of the authorisation granted to the PII owner;
- be informed by the PII owner, upon request, about the use that has been given to the PII;
- present complaints to the Superintendence of Industry and Commerce for infringements to the provisions of Law 1581 of 2012 or any other regulation that modifies, adds or complements it, after carrying out a previous consultation process or complaint with the PII owner; and
- revoke the authorisation or to request the suppression of the data when the principles, rights and constitutional or legal guarantees are not complied with by the PII owner.

39 Compensation

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?

Direct monetary compensation for breaches of the law is not contemplated in the regime. Nevertheless, in Colombia, any unlawful damage shall be indemnified. In this regard, the Constitutional Court has dictated that, pursuant to legal and constitutional provisions, data subjects may claim for damages derived from the breach of any obligation contained in the data protection regime by the PII owner or the data processor.

40 Enforcement

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

Both, as described in question 4.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Not applicable.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, the sanctions imposed by the SIC or its orders are considered administrative acts, which are subject to judicial review before the administrative jurisdiction.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

PII shall not be available online unless the PII owner undertakes adequate security measures to ensure that access is blocked to any unauthorised user.

Moreover, the use of cookies in web pages is forbidden unless the data subject has given authorisation for usage, which may be obtained by a pop-up including information about privacy policies and how to disable cookies. All other tracking systems need proper authorisation from the data subject.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Law 527 of 1999 regulates e-commerce, and hence includes the entire legislation on electronic marketing. Nevertheless, for all kinds of marketing, both electronic or mechanical, authorisation of the data subject is required.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Cloud computing services are considered a transmission of PII, where the client is the PII owner while the service provider is the data processor. In this regard, it shall comply with the obligation set forth in article 26 of Decree 1377 of 2013, as set forth in question 31. Furthermore, the service provider may outsource the services provided, in which case its contractor will be considered a data processor.

María Claudia Martínez Beltrán **mcmartinez@dlapipermb.com**

Carrera 7 No. 71-21
Tower B, Of. 602
Bogotá
Colombia

Tel: +57 (1) 3174720
Fax: +57 (1) 3174520
www.dlapipermb.com/index.php/en

France

Benjamin May and Farah Bencheliha
Aramis

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legislative framework for the protection of PII in France is one of the oldest in Europe as it is based on the Law on Computer Technology and Freedom dated 6 January 1978 (Loi Informatique et Liberté, or LIL). This law has been amended several times since then, and especially by:

- Law No. 2004-801 dated 6 August 2004 to implement the provisions of Directive 95/46/CE;
- Decree No. 2005-139 of 20 October 2005 also completes the provisions of the LIL; and
- Law No. 2016-1321 dated 7 October 2016, which anticipates the implementation of certain provisions of the EU General Data Protection Regulation.

The law on the protection of personal data, which implements the General Data Protection Regulation 2016/679 (GDPR) in France, entered into force on 20 June 2018, although some lawyers pointed out that the GDPR did not require a transposition law. This law will further amend the LIL.

Moreover, as a regulation, the GDPR has been directly effective in France since 25 May 2018.

Furthermore, the following international instruments on privacy and data protection also apply in France:

- the 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).

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

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.

Powers of sanction

The maximum threshold of penalties that the CNIL can pronounce has been increased from €150,000 to €3 million (since 25 May 2018, these thresholds have been increased to €20 million or 4 per cent of world turnover for companies in accordance with the GDPR).

The CNIL can now compel sanctioned entities to inform each data subject individually of this sanction at their own expense.

It may also impose financial penalties without prior formal notification by the bodies where the failure to fulfil obligations cannot be brought into conformity.

It can also prohibit specific processing, and erase the related personal data in case of a breach of the LIL.

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 PII and to recorded information. They can also collect information online, including under a fake identity.

The CNIL's controls are generally carried out as follows: 41 per cent stem from its own initiatives based on news released in the press, 35 per cent from its annual programme of control, 15 per cent from complaints and 9 per cent from other items.

Regulatory powers

The powers of the CNIL have recently been extended, as 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 reuse of public information available online.

3 Legal obligations of data protection authority

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

If the owner or processor of PII carries out cross-border processing either through multiple establishments in the EU or with only a single establishment, the supervisory authority for the main or single establishment acts as lead authority in respect of that cross-border processing.

As lead authority, the CNIL must cooperate with the data protection authorities in other 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 has to provide information to other data protection authorities and can seek mutual assistance from them and conduct joint investigations with them on their territories.

More generally, the CNIL is required to provide assistance to 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.

4 Breaches of data protection

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 dated 18 November 2016 for the Modernisation of the 21st Century Justice), criminal proceedings and private rights of action.

Proceedings

When the CNIL finds a PII owner to be in breach of its obligations under the LIL, as a preliminary step the CNIL chairman may issue a formal notice for the PII owner to remedy the breach within a limited period of time. 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 PII owner complies with the terms of the formal notice, the CNIL chairman shall declare the proceedings closed. Otherwise, the competent committee of CNIL may, after a contradictory procedure, pronounce one of the following penalties:

- a warning notification;
- a financial penalty, except when the PII 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 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 PII for a maximum of three months (except for certain processing carried out on behalf of the French Administration); or
- for certain sensitive files of the French Administration, the Prime Minister is given information in order for him to take the necessary measures to remedy the breaches.

In the event of a serious and immediate violation of rights and freedoms, the chairman 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 condition of bad faith 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.

Scope

5 Exempt sectors and institutions

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

The LIL is generally applicable to all public bodies and all non-public entities that process PII 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 PII by public bodies for reasons of national security is subject to a specific regime supervised by the executive power; and
- processing of PII 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 PII solely for journalistic or artistic purposes; and
- processing of PII by a natural person in the course of a purely personal or household activity.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The LIL does not cover 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.

Electronic marketing is subject to the Postal and Electronic Communication Code (article L. 34-5 et seq) and to the Consumer Code (article L. 121-20-5 et seq).

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Processing of health PII is subject to the provisions of the Public Health Code as well as to the LIL.

The solicitation by automatic calling machines, email or fax, and the sale or transfer of PII for prospecting purposes using these, is subject to the provisions of the Postal and Electronic Communications Code.

8 PII formats

What forms of PII are covered by the law?

The LIL is aimed at covering all forms of PII, 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 to the combination of one or several elements.

In addition, the LIL applies to automatic processing and to non-automatic processing of PII that forms part of a filing system (or is intended to form part of a filing system), with the exception of processing carried out for personal purposes. Accordingly, even records of PII in paper form may be subject to the LIL.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The LIL applies to processing of PII carried out by a PII owner:

- who is established in France. In this context, 'establishment' is broadly interpreted as it refers to all sorts of 'installation', regardless of its legal form; or
- who is not established in France, but who uses a means of processing located in French territory, for instance, hosting data, internet service provider, cloud services, etc.

10 Covered uses of PII

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

In principle, the LIL applies to all processing of PII, with the exception of that carried out for purely personal purposes. The controller determines the purposes for which and the means by which PII is processed,

whereas the processor processes PII only on behalf of the controller. The duties of the processor towards the controller must be specified in a contract or another legal act.

In principle, the PII 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 PII processors (including security, international transfers, 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.

Legitimate processing of PII

11 Legitimate processing – grounds

Does the law require that the holding of PII 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 PII needs to be justified under French data protection law. In principle, the ground for legitimate processing must be the consent of the data subject, but the LIL introduced statutory legal exemptions to obtain the consent of the data subject for some processing when it is carried out for the following purposes:

- 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 prior to 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.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

French law is more restrictive for the processing of specific types of PII, known as sensitive personal data. As a matter of principle, processing of sensitive data is prohibited.

The LIL provides a non-exhaustive list of sensitive PII by nature, which is PII 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 PII that has been made public by the data subject; or
- the processing is necessary for the establishment, exercise or defence of legal claims.

In relation to the use of PII in the employment context, the CNIL published several opinions on monitoring the activities of employees, video surveillance, discrimination, localisation data and collection of PII in the recruitment process. Moreover, in France, employers cannot rely on consent for processing involving PII 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 PII relating to offences, convictions and security measures, which can only be carried out by a limited number of specific entities.

Furthermore, according to the law on the protection of personal data, a minor may consent to the processing of personal data alone with regard to 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'.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? 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 PII 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 PII 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 PII and to rectify, complete, update, block or delete it if inaccurate, incomplete, equivocal or expired; and the right to direct the use of their PII after their death);
- the intended transfer of PII outside the EEA;
- 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.

14 Exemption from notification

When is notice not required?

Notice is not required if the data subject already received such information. Furthermore, in cases where the data subject did not provide his or her PII 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 with a view to protecting and promoting public health;
- the data subject already has the information;
- the PII is recorded only to comply with statutory and legal obligations; or
- the PII must remain confidential subject to an obligation of professional secrecy regulated by EU or member state law, including a statutory obligation of secrecy.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The LIL grants rights to data subjects allowing them to have some control over the use of their PII. The relevant rights in this field are notably

the right to rectify inaccurate or out-of-date PII, and the right to be forgotten, in order to obtain the deletion of such PII (see question 38).

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

As a general rule, the PII controller shall ensure that the processed PII is adequate, relevant and not excessive in relation to the purposes for which it is collected and for onward processing. In addition, the PII owner shall also ensure that PII is accurate, complete and, if necessary, updated. In this respect, the law provides that the PII 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.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

PII owners are required to limit the processing of PII to what is strictly necessary for the purpose of the processing. The amount of PII collected and processed must be proportionate to the purposes of the processing.

The LIL also provides that the PII 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 PII is collected and processed. Accordingly, if the legitimate ground of the processing has disappeared or expired, the controller should erase, anonymise or pseudonymise the PII.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The finality principle is a core principle of data protection regulation in France. PII can only be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes.

Furthermore, the CNIL already encourages PII controllers to implement the 'data minimisation' principle (which is consecrated in the GDPR), as well as the systematic use, where applicable, of anonymisation and pseudonymisation techniques.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

PII can be processed for new purposes provided that such onward processing is not incompatible with the initial purposes for which the PII was collected and subject to the data subject's rights and the principle of data minimisation.

Processing of PII for new purposes when such purposes are statistical, historical or medical research is generally considered as compatible with the initial purpose.

Processing of PII for new purposes even incompatible with the initial purpose is also possible with the prior consent of the data subject.

Security

20 Security obligations

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

Data controllers must protect PII 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 PII in their possession and control is protected from unauthorised access and use;
- implement appropriate physical, technical and organisational security safeguards to protect PII; and
- ensure that the level of security is appropriate with the amount, nature and sensitivity of the PII.

The CNIL issued guidelines on 23 January 2018 on the security measures to be implemented by data controllers, in line with the requirement of the 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 PII.

21 Notification of data breach

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 PII controllers to report PII 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 other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach; and
- describe the measures taken or proposed to be taken by the owner to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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 PII owner must keep an updated record of all PII 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 PII to an administrative fine of up to €10,000,000 or, in 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 PII breach. In this respect, when the PII breach may affect PII or the privacy of a data subject, the PII controller shall also notify the concerned data subject without delay.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

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 the PII. In a nutshell, 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.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

PII controllers are required to maintain a record of processing activities under their responsibilities as referred to in article 30 of the GDPR. Processors of PII 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 PII 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.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Since the GDPR is directly effective in France, controllers and processors of PII 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.

In addition, 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 privacy impact assessment (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 (see question 22).

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

PII controllers or processors are not required to register with the CNIL.

Since the entry into force of the GDPR, owners and processors no longer have the obligation to declare the PII processing they carry out to the CNIL.

However, the law on personal data maintains the requirement of a prior authorisation from the CNIL for three types of processing:

- of biometric or genetic data by the state;
- for research, study or evaluation in the field of health; or
- of social security numbers.

26 Formalities

What are the formalities for registration?

The formalities are free of charge and can be realised on the CNIL's website and are non-renewable since they remain valid for the whole duration of the processing.

The formalities of registration must be performed for each new PII processing operation.

For data processing requiring prior authorisation, the following information must be provided:

- the identity and the address of the data controller;
- the purposes of the processing and the general description of its functions;
- if necessary, the combinations, alignments or any other form of relation with other processing;
- the PII processed, its origin and the categories of data subjects to which the processing relates;
- the period of retention of the processed information;
- the department responsible for carrying out the processing;
- the authorised recipients to whom the data may be disclosed;
- the function of the person where the right of access is exercised, as well as the measures relating to the exercise of this right;
- the steps taken to ensure the security of the processing and data, the safeguarding of secrets protected by law and, if necessary, information on recourse to a sub-contractor; and
- if applicable, any transfer of PII that is envisaged outside of the EEA.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Failure to comply with the registration obligation can be punished by imprisonment for a maximum period of five years and a criminal fine of up to €300,000 (article 226-16 and 226-16-1 A of the Criminal Code).

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

For processing subject to the prior authorisation procedure, the CNIL can refuse its registration if some of the information to be provided is missing or if the PII collected for the processing is too broad in relation to its purpose. In such cases, the PII owner cannot carry out the intended data processing. Failure to comply with a refusal of the CNIL to authorise processing is subject to criminal sanctions (see question 27).

29 Public access

Is the register publicly available? How can it be accessed?

On 30 August 2017, the CNIL published on its website a register that lists the formalities completed since 1979 by data controllers (public and private). This register can be consulted freely, with ease, via the CNIL website.

30 Effect of registration

Does an entry on the register have any specific legal effect?

As regards processing subject to the prior authorisation of the CNIL, the PII owner may only be allowed to start carrying out the processing upon registration and receipt of authorisation from the CNIL.

The registration as such does not exempt a data controller from any of its other obligations. After the registration, data controllers still need to ensure that the processing complies with the information disclosed in the notification and with data protection standards.

31 Other transparency duties

Are there any other public transparency duties?

Not to our knowledge.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the LIL regime, any person that processes PII on behalf of the data controller is regarded as a processor. The processor may only process PII under the data controller's instructions.

When a data controller outsources some of its processing or transfers PII in relation with such processing to a sub-contractor (ie, a data processor), it must establish an agreement with the said processor.

This agreement shall 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.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Generally, there are no specific restrictions on the disclosure of PII other than the general data protection principles provided by the LIL.

Nevertheless, disclosure of sensitive PII 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 PII.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

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

Such transfers of PII from France are permitted to Canada (under certain conditions), Switzerland, Argentina, Guernsey, the Isle of Man, Jersey, the Faroe Islands, Andorra, Israel, Uruguay and New Zealand.

Furthermore, transfers of PII from France to recipients established in the US are permitted to the extent that they are registered under the Privacy Shield certification.

Transfers of PII to other countries, or to recipients in the US who have not chosen to sign up to the Privacy Shield, are prohibited unless:

- the data subject has expressly consented to its transfer; 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 of pre-contractual 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.

When the data subjects' consent cannot be collected for any reason but notably in the hypothesis of employment relationships, the following alternative solutions are likely to ensure an adequate level of compliance:

- standard contractual clauses (SCCs) – model clauses designed by the European Commission to facilitate transfers of personal data from the EU to all third countries, while providing sufficient safeguards for the protection of individuals' privacy; and
- binding corporate rules validated by the CNIL.

Data controllers must inform data subjects of the data transfer and provide the following information:

- the country where the recipient of the data is established;
- the nature of the data transferred;
- the purpose of the transfer;
- categories of the recipients; and
- the level of protection of the state concerned or adopted alternative measures.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Unless the cross-border data transfer is based on standard contractual clauses, such transfers are subject to the same notification regime as the data processing itself (see question 26).

When the cross-border transfer is grounded on SCCs, the transfer must be approved by the CNIL. In practice, the CNIL does not require to be provided with the SCCs unless the data exporter and the data recipients have amended them.

36 Further transfer

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 PII owner based in France to a data processor outside of the EEA. 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.

Rights of individuals

37 Access

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

Data subjects have a right to 'access' the PII 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 PII owner provides the following information:

- confirmation as to whether the controller processes the data subject's PII;
- information related to the purposes for which the PII is processed, and the recipients or categories of recipients to whom the PII 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; and
- information allowing the data subject to know and to contest the logic underlying the automated processing in the event of a decision taken on the basis of it and producing legal effects with regard to the person concerned.

The controller may oppose manifestly abusive access requests, in particular with respect to 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 PII 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 PII is pseudonymised or anonymised) and for a period not exceeding what is necessary for the sole purpose of statistical, scientific or historical research.

38 Other rights

Do individuals have other substantive rights?

In addition to the right of access described above, data subjects are granted the rights described below. When PII 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 PII 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 PII related to them for the purposes of direct marketing by the PII owner or by an onward data controller.

Right to correct
Upon proof of their identity, data subjects may require the PII 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 PII has been transmitted to a third party, the data controller must carry out the necessary diligence to notify such third party of the modifications operated in accordance with the data subjects' request.

Right to be forgotten
Data subjects have the right to request the PII 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 PII is no longer necessary in relation to 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 PII has been unlawfully processed;
- the PII has to be erased for compliance with a legal obligation in EU or member state law to which the controller is subject; or
- the PII has been collected in relation to the offer of information society services.

Right to be forgotten for children
Data subjects have the right to request the PII 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 under age at the time of collection. When the PII controller has transmitted the concerned data to another PII owner, the data controller shall take reasonable measures, including technical measures, to inform the onward PII 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 in the exercise of the public authority entrusted to the controller;
- to public health;
- to archival purposes of public interest, for scientific or historical research or for 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.

39 Compensation

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 LIL that qualifies as a criminal offence subject to the referral to criminal jurisdiction.

In this case, compensation may amount to the total amount of damage endured by the individual, which includes moral damages or injury to feelings.

40 Enforcement

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

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Not applicable.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

PII owners can appeal against orders or sanctions pronounced by the CNIL in front of the Supreme Court for the administrative order (the Council of State).

Specific data processing

43 Internet use

Describe 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. Such consent may derive from the browser or other application settings. 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.

As regards analytics, the CNIL considers that these cookies may be exempted from prior consent subject to the following:
- information must be given to users who must be able to oppose processing (this opposition must be possible from any terminal);
- the data collected must not be cross-checked with other processing (client files or statistics of attendance of other sites, for example);
- the cookies must be used only for the purpose of anonymous statistics and should not allow the tracking of navigation on different sites;
- raw attendance data associating an identifier must also not be retained for more than 13 months; and
- the use of an IP address to geolocate the user should not allow the street to be determined: only the first two bytes of the IPv4 addresses can be preserved and possibly used for geolocalisation (for IPv6 only the first six bytes can be retained).

Implied consent is now accepted and companies must implement a two-step approach for obtaining consent.

Data controllers must use a banner providing the following information to the website user:

- purposes of the cookies;
- the possibility to object to the use of cookies and to modify settings by clicking on a link (made available in the cookie banner). Such link must describe the operations to be carried out by the data subject to disable the cookies;
- that further navigation on the website constitutes valid consent to the storage of cookies on their device; and
- an explanation of how disabling cookies might affect the data subject's use of the website or app.

The CNIL recommends that to ensure that the data subject's consent is unambiguous, the banner shall not disappear until the individual continues to navigate on the website, for example, by clicking on an element of the website or navigating to another page of the website.

The CNIL considers that the consent given by the data subject is only valid for 13 months. After this period, the consent of data subjects shall be collected again with the same conditions. Accordingly, the cookies' lifetime shall be limited to 13 months from the date of the first deposit on the user's device. New visits of the user to the website shall not automatically extend the cookies' lifespan.

In addition, data subjects shall be provided with an easy way to withdraw their consent to the deposit of cookies at any time.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

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
- 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 in accordance with 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 B2B 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 has the possibility to 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 in relation to the recipient's profession.

Direct marketing by regular mail or telephone is not subject to the prior consent of the recipient, but the recipient has the possibility to 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.

45 Cloud services

Describe 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 dated 25 June 2012. These guidelines contain seven recommendations by the CNIL that should be taken into account 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 with respect to 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.

Aramis

Benjamin May **may@aramis-law.com**
Farah Bencheliha **bencheliha@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

Germany

Peter Huppertz
Hoffmann Liebs Fritsch & Partner

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Primarily, data protection in Germany is governed by the EU General Data Protection Regulation (GDPR) entering into force on 25 May 2018, as standardised European law. However, as the GDPR includes specific opening clauses and allows national legislators an individual set of rules for particular areas via these clauses, there will still be a national data protection law in Germany. This national data protection law, for instance, data protection in the context of employment, is governed by the Federal Data Protection Act (the Act).

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

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. In order 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 €20,000,000 or 4 per cent of annual turnover).

3 Legal obligations of data protection authority

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

On a regular basis, the DPAs of the German federal states come together as the *Datenschutzkonferenz* (DSK) and publish concerted opinions on controversial issues. European DPAs have a similar association in the Article 29 Working Party, which publishes concerted opinions on a regular basis as well. The GDPR further provides for a One Stop Shop, allowing data controllers to coordinate cross-border processing activities in Europe with only one leading DPA.

4 Breaches of data protection

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 (UWG) (violation of business secrecy).

Breaches may also be fined. The GDPR provides for a graduation of 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 €10,000,000 or 2 per cent of annual turnover; and
- serious breaches with an administrative financial penalty of up to €20,000,000 or 4 per cent of annual turnover.

Scope

5 Exempt sectors and institutions

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

The GDPR is generally applicable to all federal public authorities, state public authorities and all non-public entities that process PII. However, the GDPR is subsidiary to various area-specific rules, which make a number of authorities or entities subject to special regulations.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The GDPR does not cover interception of communications, which is addressed in other special regulations such as the German Code of Criminal Procedure (StPO) and the German Code of Telecommunications (TKG). Electronic marketing is covered only partially by the GDPR. The UWG holds additional and more comprehensive provisions regarding this. Monitoring and surveillance of individuals is also covered by the StPO. In this regard it is complemented by corresponding acts on the police authorities of the individual federal states.

7 Other laws

Identify 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 worth noting here in particular is the TKG, which provides comprehensive area-specific rules on telecommunication services.

8 PII formats

What forms of PII are covered by the law?

The GDPR does not show any significant limitations to the scope of PII. So 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 DPAs and case law, even email and IP addresses fall under PII.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

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 (EEA). Under certain conditions the GDPR may also be applicable to data controllers outside the EEA, 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 EEA; or
- monitors their behaviour as far as their behaviour takes place within the EEA.

10 Covered uses of PII

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

Basically all processing or use of PII is covered by the GDPR as it follows a model in which every processing or every use of PII has to be justified. With respect to 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 (see question 20). The responsibility for data controllers and mere data processors differs under the GDPR, even though data processors have a quite comprehensive responsibility on their own.

Legitimate processing of PII

11 Legitimate processing – grounds

Does the law require that the holding of PII 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 PII needs to 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 in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject; 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 personal data, in particular where the data subject is a child (ie, the balance of interest test).

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

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. With respect to data processing for business purposes, this is allowed when, for example:

- it 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 ;
- 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 which 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 PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? 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: identification of the data controller; contact of data protection officer; the purposes of processing; the legal basis for the processing; the legitimate interests; the recipients or categories of recipients; and the intention to transfer PII to a third country.

Additional information may be necessary, depending on the circumstances, in order to ensure lawful and proper processing. It is recommended that such a more complete notice is provided to the affected data subjects, since this will enhance trust in the processor's information practices.

If PII 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.

14 Exemption from notification

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 PII would affect legal claims of the data controller; or
- PII was acquired from generally accessible sources and notification would require a disproportionate effort.

In addition to the above there are a few more exemptions, which follow either further legal obligations to keep data or the collection from publicly available data sources.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The GDPR provides individuals the rights to rectify, erase and restrict PII. Besides this, it does not provide individuals with any degree of choice or control over the use of their PII. This is not necessary because, in general, the consent of individuals has to be obtained to process their data unless one of the legal permissions is applicable.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

As a general rule, appropriate steps must be taken to ensure correctness and accuracy for the purposes for which personal data is obtained and processed.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

As a general rule, the amount of PII 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 due to his or her particular personal situation override the interest of the controller in such collection, processing or use or for the establishment, exercise or defence of legal claims; or in specific cases where PII is processed for advertising purposes.

Instead of ceasing, the GDPR normally demands blocking PII in the event that 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 cases of exception, such as a risk to life or limb (risk of terrorism)); and in connection with any data processing for advertising purposes. When summarised, PII 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.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

PII must be adequate, relevant and not excessive in relation to the purposes for which it is processed.

PII 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.

PII 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 with the aim of collecting, processing and using as little PII 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.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The finality principle is adopted in German statutory data privacy regulations. As the purpose of any further data processing or use has to be determined with collecting PII, 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 PII follow special rules for justification in the GDPR.

Security

20 Security obligations

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

The data controller must implement appropriate technical and organisational measures to protect PII against loss or any form of unlawful processing (including theft, unlawful copying or recording). These measures must guarantee an appropriate level of security, taking into account 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 PII.

The GDPR provides for the following security measures in particular to be taken into account:

- 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 in a timely manner 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 furthermore 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 taken into account. Additionally, the data controller is required to select only third-party service providers that offer adequate guarantees for technical and organisational information security.

21 Notification of data breach

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 PII 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 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, notification may be replaced by a public communication, or other means that would provide equivalent exposure in view of 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, 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 data protection officer, the proposed measures to limit possible negative consequences and the likely consequences of the unlawful disclosure.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The appointment of a data protection officer (DPO) is mandatory if:

- the controller carries out automated processing with at least 10 employees;
- the core activities of the controller consist of processing operations which, by virtue of 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 PII or PII 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 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 a 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 day-to-day administration of privacy complaints and supervision and handle any prior checking, including for international transfers and sensitive data processing.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Individuals have a right to request detailed information about what data of theirs is processed and how it is processed (see question 37). The owners of PII have to comply with all such requests every time. Therefore, the owners 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 (see question 22), the data owner still has to 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).

24 New processing regulations

Are there any obligations in relation to new processing operations?

The GDPR provides for specific obligations to establish data protection by design and 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, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR. The controller shall further implement appropriate technical and organisational measures for ensuring that, by default, only PII which is necessary for each specific purpose of the processing is processed. Where a type of processing in particular using new technologies, and taking into account 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, prior to the processing, also carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (data protection impact assessment).

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There is no general requirement to register with the DPA. The DPO's contact details, however, must be submitted to the DPA. The controller shall make its internal register of processing operations available to the DPA on request.

26 Formalities

What are the formalities for registration?

The form for notifications to the DPA can be submitted in writing or via email or fax. There are no fees for notification.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

No penalties apply.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

There is no such instrument for the DPA to to refuse an entry on the register.

29 Public access

Is the register publicly available? How can it be accessed?

There is no public register.

30 Effect of registration

Does an entry on the register have any specific legal effect?

No legal effect is connected with this.

31 Other transparency duties

Are there any other public transparency duties?

No such public transparency duties apply, except for the notification obligations in case of personal data breaches (see question 21).

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Outsourced processing services will mostly be considered 'contract data processing on behalf' under the GDPR. The conditions shown under question 20 apply to this kind of data processing. But 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, as shown in questions 11 and 33.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

The term 'disclosure' is not defined in the GDPR, but relates to making PII public and transferring PII 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 as mentioned in question 11, and such disclosure is not incompatible with the purposes for which the PII was initially collected.

As the GDPR does not include an affiliated company privilege, every transfer of PII between two legally independent companies (including company group member entities) has to be justified, meaning by laws, consent or company agreement; this particularly applies if the receiving company has a registered office in a non-EEA country.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Transfers outside the EEA 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 EEA are not subject to such restrictions other than those mentioned in question 33.

Transfers of PII outside the EEA 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 ongoing data streams are still the 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 ECJ's judgment invalidating the US Safe Harbor Agreement (which was a former instrument for data transfers to the US).

With respect to data transfers to the US, the US Safe Harbor Agreement is replaced by the EU–US Privacy Shield. This provides one more instrument for data transfers to the US. As of 1 August 2016, US companies can register under this agreement.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No such duty of notification applies. From a legal point of view the DPA is not entitled to authorise data transfers. However, in practice it will be very helpful to arrange things with the DPA to avoid sanctions in the future.

The DPA is competent for authorisation of the transfer only with respect to a potential data transfer in foreign countries with no adequate level of data protection. In legal terms, the authorisation is still limited to the selection of the target country, so justification of the transfer itself remains unaffected (see questions 11 and 33).

36 Further transfer

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 (see question 32) 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.

Rights of individuals

37 Access

Do individuals have the right to access their personal information held by PII 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 PII undergoing processing. Access needs to be provided in writing or in 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 (such as 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);
- PII 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
- PII 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.

38 Other rights

Do individuals have other substantive rights?

Individuals have the following rights:

- to be informed (notice requirement);
- to request to rectify, supplement, delete or restrict PII relating to them that is inaccurate, incomplete or irrelevant for the purposes of the processing, or is being processed in any other way that infringes a legal provision;
- to object to processing of their PII if the processor bases the processing of PII on its proper legitimate interests (which do not outweigh the individual's privacy), which may be the case if the processor plans to provide PII to a third party or for processing of PII for the purpose of marketing;
- to receive the PII 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 compensation if they suffer damage or distress as a result of a breach of the GDPR or other data protection provisions.

Update and trends

The two big issues being discussed are the responsibility of data controllers for the data processing of social media platforms when using a social media page and the requirements for using cookies on websites for tracking and retargeting users. Following the Facebook ruling of the CJEU, German DPAs have set up strict requirements for these processing operations. It will be interesting to see how these requirements will be enforced and if they will be upheld by the courts.

39 Compensation

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?

With regard to 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.

40 Enforcement

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

The DPA is only entitled to control the provisions of the GDPR and other data privacy regulations. It can punish the data owners 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

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Alongside the limitations already shown above and the special limitations of area-specific rules, the GDPR provides some distinctive provisions for children's consent to processing of special categories of PII, processing of PII relating to criminal convictions and processing that does not require identification.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Fines imposed by the DPA can be revised by the ordinary courts. Legal protection and remedies against any other orders of the DPA can be filed with the DPA itself or with the German administrative courts if the DPA fails to remedy the concern.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The legal use of cookies is currently under discussion, because the relevant EU 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 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 Article 29 Working Party, the various types of cookies should be distinguished. However, in all cases, the website's privacy policy should contain a description of how the PII is processed. Additionally, the cookie provider should grant the individual an opportunity to object against the use of the PII.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

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. In the event that such objection is registered, the sender must take all steps to stop sending commercial messages by using the 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 for the purposes of being 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 EEA and the sender has fulfilled all provisions in that country with respect to the sending of unsolicited communications.

45 Cloud services

Describe 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 has to meet all requirements for assigning data processors as already set out in question 20. Moreover, the DPAs 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 (see question 34), 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 with respect to the location of data processing, notification about changes in the location, and portability and interoperability of the data in case of, for example, 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 in order to safeguard information security, portability and interoperability of data.

HOFFMANN LIEBS FRITSCH & PARTNER
RECHTSANWÄLTE mbB

Peter Huppertz **peter.huppertz@hlfp.de**

Kaiserswerther Straße 119
40474 Düsseldorf
Germany

Tel: +49 2 11 5 18 82 1 97
Fax: +49 2 11 5 18 82 2 20
www.hlfp.de

Greece

Vasiliki Christou
Vasiliki Christou

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Until 25 May 2018, Law 2472/1997, a dedicated data protection law transferring Directive 95/46/EC was in force. After entry into force of the General Data Protection Regulation 2016/679/EE (GDPR) on 25 May 2018, which prevails over statutory law, Law 2472/1997, although not yet abolished, may not be enforced in areas regulated by the GDPR. Moreover, a law implementing the GDPR and transferring Directive 2016/680 has been submitted to public consultation. The consultation is closed but the law has not been issued yet. In this chapter this draft law will be briefly mentioned as the law under preparation. The European Convention of Human Rights is also applicable in Greece, prevailing over statutory law, but not over the GDPR.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The responsible authority is the Greek Data Protection Authority. The Greek Data Protection Authority may perform investigations, either on its own initiative or after a complaint has been lodged, and obtain access to the premises of a PII owner or processor, including data protection equipment and means, as well as personal data and all information necessary for the performance of its tasks.

Moreover, the Greek Data Protection Authority has the power to order the PII owner or the PII processor to provide any information it deems necessary, to carry out investigations in the form of data protection audits and to carry out reviews on certifications related to data protection. According to the law under preparation implementing the GDPR (see question 1), every public authority has to assist the Greek Data Protection Authority in the performance of its tasks. Additionally, the members of the Greek Data Protection Authority and specially authorised secretary employees have investigative powers applicable in criminal processes and need no warrant to perform an investigation.

3 Legal obligations of data protection authority

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

The Greek Data Protection Authority, like all supervisory authorities in EU member states, participates in the 'consistency mechanism' provided in the GDPR. Therefore the Greek Data Protection Authority is under the obligation to cooperate with, including sharing information and providing mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of the GDPR. The Greek Data Protection Authority shall also participate in joint operations, joint investigations or joint enforcement measures of the supervisory authorities. To resolve disputes between supervisory authorities, the European Data Protection Board shall issue binding decisions, which may be challenged before the European Court of Justice.

4 Breaches of data protection

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

Breaches to data protection law shall lead to administrative sanctions, imposed by the Greek Data Protection Authority, as well as to criminal penalties imposed by the criminal courts.

Scope

5 Exempt sectors and institutions

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

National security and policing do not fall under the scope of the GDPR, but they do fall under the scope of Directive 2016/680/EU, which is transferred to the Greek legal order by the law under preparation mentioned in question 1.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Interception of communications is covered by Law 2225/1994 on freedom of communication, which implements article 19 of the Greek Constitution providing for the right to communication privacy. Articles 370 and 370A of the Greek Penal Code concerning the privacy of correspondence, telephone conversations and oral conversations also apply. As regards the interception of electronic communications, article 4 of Law 3471/2006 implementing Directive 2002/58/EC on electronic communications privacy applies as well. Law 3115/2003 establishes the Greek Communications Security Authority, which is responsible for supervising the security of communications infrastructure.

Electronic marketing or monitoring is covered by Law 3471/2006, implementing Directive 2002/58/EC on electronic communications privacy. For any issue not covered by Law 3471/2006, the GDPR applies. Law 3471/2006 will be abolished once the ePrivacy Regulation comes into force.

CCTV is covered by the GDPR, and the law under preparation implementing the GDPR (see question 1) includes special provisions on the use of CCTV. Also, the Greek Data Protection Authority issued, under the force of Directive 95/46/EC and Law 2472/2007, Directive 1/2011 on the use of CCTV in private or semi-private entities (eg, restaurants, banks, etc) and Directive 115/2001 on the protection of privacy in the workplace, also dealing with the issue of CCTV. Notwithstanding the GDPR, these two directives may still be consulted.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

In addition to the laws and regulations listed in question 6, the following specific data protection rules should also, indicatively, be pointed out:

- Legislative Decree 1059/1951, as in force, on bank account privacy;
- article 40 of Law 3259/2004, as in force, on the retention period of data relating to economic behaviour;
- Law 3691/2003, as in force, concerning anti-money laundering measures, in combination with Law 3932/2011 on the establishment of an anti-money laundering authority;
- decisions of the Greek Data Protection Authority (Nos. 109/1999, 523/1999, 86/2002, 24/2004, 6/2006, 11/2006, 21/2007 and 50/2011) on data processing by TEIRESIAS SA, a société anonyme responsible for the holding of data concerning legal or natural persons in default, bankruptcy, etc;
- article 5 of the Administrative Procedure Code, as in force, regarding access to documents;
- Law 3861/2010, as in force, on open governance; and
- Law 3979/2011, as in force, on electronic governance.

8 PII formats

What forms of PII are covered by the law?

Both automated and non-automated processing activities are covered by the law, but personal data should be structured according to specific criteria that composes a filing system.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Based on article 3 of the GDPR, it is applied to both PII owners and PII processors established in Greek territory, as well as to data subjects in Greece that have been offered goods or services or whose behaviour is monitored by PII owners or PII processors not established in the EU.

10 Covered uses of PII

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

All processing or use of PII is covered.

A distinction is made between PII owners and PII controllers, but a PII owner is also a PII controller and bears the duties of a PII controller.

The duties of PII owners and controllers on the one hand and PII processors on the other hand differ accordingly. PII owners and controllers bear the full bundle of obligations, provided for by the GDPR, indicatively they are responsible for:

- lawfully processing personal data, eg, after acquiring the explicit consent of the data subject;
- accommodating and satisfying the data subjects' rights (to information, access, rectification, erasure, restriction of processing, data portability and the withdrawal of consent);
- notifying the Data Protection Authority of a data breach;
- conducting a data protection impact assessment (DPIA) study, if applicable; and
- providing documented instructions to processors on data processing in a data processing agreement with the processor.

Processors are mainly responsible for:

- fulfilling their contractual obligations under the data processing agreement, and informing the PII owner or controller if an instruction, in their opinion, infringes the GDPR or other data protection law;
- notifying the PII owner or controller of a data breach;
- assisting the PII owner or controller in answering data subjects' requests, and in satisfying their rights, if possible and reasonable;
- at the request of the PII owner or controller, deleting or returning all PII after the end of the provision of services, and deleting existing copies, unless the law requires otherwise;
- ensuring that their personnel have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
- making available to the PII owner or controller all information necessary to demonstrate compliance with their obligations; and
- allowing for and contributing to audits, including inspections, conducted by the PII owner or controller or another auditor mandated by the latter.

Legitimate processing of PII

11 Legitimate processing – grounds

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

PII holding has to be legitimised on the following specific grounds:

- consent;
- performance of a contract (eg, to proceed to payments or other obligations in the contract) or a precontractual stage necessitating the collection of PII (to conduct due diligence);
- compliance with a legal obligation of the PII owner, eg, imposed by tax legislation, labour law or a court order in the course of a criminal investigation;
- protection of the vital interests of a data subject (eg, health) or of another natural person; or
- protection of the legitimate interest of the PII owner or a third party (for example with whom the PII owner has a contractual relationship) that is not overridden by the rights and interests of the data subjects.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Processing of personal data revealing racial or ethnic origins, 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 in principle prohibited.

The processing of such data is exceptionally permitted if:

- an explicit consent is available, unless consent is not the legal basis for processing;
- the vital interests of the data subject or of another natural person are concerned, and the data subject is physically or legally incapable of giving consent;
- a substantial public interest specified by law is at stake;
- it is necessary to defend a legal claim;
- it is necessary for reasons of public health;
- personal data has been manifestly made public by the data subject; or
- it is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Specific types of data related to beliefs may be processed by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim in the course of their legitimate activities, 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.

Additionally, specific safeguards apply to employees' data, health and genetic data, and data relating to criminal convictions and offences.

With regard to employees' data, it will be possible to process even specific types of data under the following main safeguards, which are currently included in the law under preparation implementing the GDPR (see question 1):

- processing has to be necessary for the fulfillment of a specific obligation of the employer or the employee deriving from an employment contract or from labour law, including obligations related to hygiene and safety at work, as well as social security legislation;
- health data may be obtained from the employee only if it is absolutely necessary to evaluate suitability for a job, and for the

recognition of social benefits to the employee. Health tests, including psychometric and psychological tests, are only permitted under special circumstances in connection with specific duties demanding such an evaluation;
- processing of genetic data is not permitted. It might be permitted based on a specific law under strict conditions and after prior consultation with the data protection authority;
- processing of data relating to criminal convictions or offences is possible if it is absolutely necessary for a specific job and may be obtained only after the individual has given his or her written consent; and
- processing of biometric data is possible if it is absolutely necessary for safety reasons in connection with the special circumstances of a specific working environment.

As regards health data, according to the law under preparation implementing the GDPR (see question 1), explicit and written consent is always required prior to processing.

For genetic data, according to the law under preparation implementing the GDPR, the processing as well as the performance of genetic prognostic tests is forbidden for the purposes of life and health insurance.

According to the law under preparation implementing the GDPR, data related to criminal convictions or offences may be processed mainly under the following circumstances:
- if it is necessary based on a provision of law to be selected for a job;
- to exercise freedom of expression;
- for archiving purposes in the public interest;
- for statistical, scientific and historic research purposes; or
- to defend a legal claim.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Yes, the PII owner must notify the individual whose PII it holds. If PII is collected from the data subject, then the notification must be made at the time of the collection. If PII is collected from another source, then the notification must take place within a reasonable period after collection depending on the circumstances, and in any case not exceeding one month, or at the time of the first communication with the data subject, if the PII is to be used for that purpose, or prior to a disclosure to another recipient, if PII is to be used for such a purpose.

The notification must contain:
- the identity and contact details of the PII owner and the contact details of the DPO, if applicable;
- the purposes and the legal basis of processing. If the legal basis for processing is a legitimate interest of the PII owner, the PII owner must explain the legitimate interest. If the legal basis is a statutory, contractual or pre-contractual obligation, the PII owner has to explain such an obligation, and also the consequences, in case of failure to provide such data;
- the retention period or the retention criteria;
- the eventual recipients and data transfers. If PII is transferred outside the EU, the PII owner has to explain whether the PII is transferred to an organisation covered by an adequacy decision or not. If not, the PII owner has to demonstrate the appropriate safeguards governing such a transfer and offer the ability to have a copy of them;
- the data subjects' rights (access, rectification or erasure of personal data, restriction of processing concerning the data subject and objection to processing, as well as the right to data portability and the ability to withdraw consent, if applicable), including the right to lodge a complaint before the supervisory authority; and
- if PII has not been obtained from the data subject, the PII owner has to inform the data subject about the source of the PII, as well as whether it came from a publicly available source.

14 Exemption from notification

When is notice not required?

A notification is not required if the data subject already has all the information required and the PII owner is able to demonstrate such fact, eg, if all the required information has been provided before acquiring consent to data processing.

Additionally, if PII has been obtained by a source other than the data subject, then notification is not required if it is impossible, would demand disproportionate effort or would make impossible or impair seriously the objectives of the processing; or if the PII must remain confidential due to professional or statutory secrecy obligations.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

As a principle, individuals are entitled to provide their consent to the processing of any personal data concerning them. That means that the individual freely (that is, without any coercion or fear of the consequences) gives a specific (that is, related to a particular purpose), informed and unambiguous indication of his or her wishes, by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Additionally, PII owners must offer individuals the ability to withdraw their consent to processing in the future as easily as the consent was given.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Not specifically.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

PII may be kept for as long as it is necessary to serve the purpose of processing. No specific retention period is laid down in the GDPR or the law under preparation implementing the GDPR (see question 1).

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes, the finality principle applies.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Further processing is exceptionally permitted in the following cases:
- if the data subject has given his or her consent to the processing for a specific purpose other than that for which the personal data has been collected;
- if a law that is both necessary and proportionate in a democratic society provides for such an exception in order to safeguard important aspects of the public interest, such as national security, defence, public security, 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, an important economic or financial interest of the EU or a member state, the protection of judicial independence and judicial proceedings, the enforcement of civil law claims, etc;
- for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes, under the condition that such further processing does not permit or no longer permits the identification of data subjects; or
- if the PII owner can ascertain compatibility of the initial purpose with the further purpose, taking into account any link between

them, the context in which the PII has been collected, in particular regarding the relationship between the data subjects and the PII owner, the nature of the personal data (if it is simple or sensitive), possible consequences for the data subjects and the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Security

20 Security obligations

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

The PII owner has to follow technical and organisational security measures, which are generally prescribed in the GDPR by reference to:

- pseudonymisation and encryption;
- ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the security of the processing.

Directive 2016/680/EU specifies the security measures as those designed to control equipment access, data media, user, data access, communication, input and transport, as well as recovery and integrity measures.

The Greek DPA published on its website under the force of Law 2472/1997 a detailed template of a security policy, incorporating suggestions and directions for technical and organisational measures, physical and electronic security measures and a restoration plan in case of an accident. This template may still provide some guidance to PII owners.

For electronic communication services providers, the Communications Security Authority has issued decisions (eg, Government Gazette 1742/B/2013, Government Gazette 2715/B/2011) that include analytic provisions about what a security policy (based on the details of the processing) should include. Such provisions are strictly enforced by the Communications Security Authority.

As the NIS Directive (the directive on security and information systems) entered into force on 9 May 2018, a Greek law implementing the NIS Directive and eventually prescribing certain security measures or a certain level of security for digital services providers is anticipated.

A PII owner has to carry out an assessment of the impact of the envisaged data processing when the processing is likely to result in a high risk to the rights and freedoms of natural persons. For the preparation of a DPIA, the PII owner has to consult the Greek Data Protection Authority.

21 Notification of data breach

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 case of a personal data breach, the PII owner has to notify the Greek Data Protection Authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal 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, it shall be accompanied by reasons for the delay.

The PII owner also has to notify the data subject of the data breach without undue delay when the personal data breach is likely to result in a high risk to his or her rights and freedoms. The PII owner is not under an obligation to inform the data subject if:

- appropriate technical and organisational protection measures, such as encryption, have been applied;
- subsequent measures mitigating the high risk to the rights and freedoms of data subjects means it is no longer likely to materialise; or
- it would involve disproportionate effort. In such a case, a public communication or similarly effective measure takes place instead.

However, the Greek Data Protection Authority may still demand that the data subject be notified.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The appointment of a data protection officer is mandatory for the public sector, including administrative authorities of the state, legal entities of public law and state-owned legal entities offering products or services of public goods or operating infrastructure facilities.

As regards the private sector, the appointment of a data protection officer is mandatory if the data processing involves regular and systematic monitoring of data subjects on a large scale, eg, for the purposes of behavioural advertising or for safety reasons as in the case of CCTV. The appointment of a data protection officer is also mandatory if the core activities of the controller or the processor consist of processing on a large scale of special categories of data (eg, health data) or data relating to criminal convictions and offences.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Both PII owners and controllers are required to maintain records of processing activities under their responsibilities in writing, including in electronic form, which shall be made available to the Data Protection Authority upon request.

PII owners and controllers are exempted from such an obligation if they employ fewer than 250 persons. However, the exemption does not apply if the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional or the processing involves sensitive data or data relating to criminal convictions and offences.

24 New processing regulations

Are there any obligations in relation to new processing operations?

A DPIA must be carried out with regard to new processing operations or existing processing activities that change significantly and meet the criteria for high-risk processing laid down by article 35 GDPR.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

After 25 May 2018, PII owners or processors are not required to register with the supervisory authority. No exemptions have been made so far.

26 Formalities

What are the formalities for registration?

Not applicable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

No, there are not.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

If the entity is within the EU or is covered by an adequacy decision of the European Commission (that is, a decision of the Commission ascertaining an adequate level of data protection in the third country in question), then data transfer shall be governed by a written contract, namely a data processing agreement between the PII owner and the entity, which is in this case the data processor. The data processing agreement shall include the following content:

- the documented instructions of the PII owner regarding the categories of data to be processed, the categories of data subjects concerned, the scope and the duration of processing;
- technical and organisational security measures;
- the obligation of the data processor to ensure that processing personnel are bound by confidentiality, and ensure that sub-processors are contractually bound to abide by the same level of data protection as specified in the data processing agreement;
- a list of sub-processors approved by the PII owner. If this list changes, the sub-processor must be contractually bound to notify the PII owner first and give him or her the right to object; and
- other obligations listed under question 10.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Restrictions of disclosure to other recipients may be derived from professional or statutory secrecy obligations.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

If the entity receiving personal data (either another PII owner or a PII processor) is outside the EU and is not covered by an adequacy decision, then data transfer shall be subject to appropriate safeguards and governed by standard contractual clauses between the data importer and the data exporter providing for such safeguards. The issuance of model standard contractual clauses (SCCs) by the European Commission is anticipated. In the absence of such 'official' model SCCs, data exporters need to execute SCCs with the data importers, which will have been approved by the Greek Data Protection Authority in the course of an authorisation process.

In special situations some derogations from the aforementioned restrictions are applicable, namely:

- if the data subject has explicitly consented to the transfer after being informed of the risks involved;
- the transfer is necessary for the performance of a contract between the data subject and the data exporter or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data exporter and a third person (eventually the data importer);
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Update and trends

Issues dealt with herein must be reviewed when (i) the draft law implementing the GDPR and Directive 2016/680 is issued; (ii) the ePrivacy Regulation is issued; and (iii) a directive for the protection of persons reporting on breaches of EU law (whistle-blowers) is issued.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Yes, an authorisation is required if:

- cross-border transfer concerns an organisation not covered by an adequacy decision; and
- no model SCCs have been issued by the European Commission.

36 Further transfer

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

Yes, all onward transfers have to satisfy the same level of data protection.

Rights of individuals

37 Access

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

Individuals have the right to access personal data held by PII owners. This means they may be able to get a hard or an electronic copy (depending on the circumstances) of the personal data held by the PII owner, and that they become aware of the conditions of the processing, eg, its scope and purposes and the retention period, as well as conditions for data transfer to other recipients and third countries. For further copies of personal data held, a reasonable fee may be charged.

The access right may be exercised by filing an application or sending an email to the PII owner or the data protection officer.

Limitations to this right may be foreseen by the law to safeguard important public interests such as national security and defence, monetary crises, the secrecy of criminal investigations, etc.

Also, limitations are foreseen in cases of processing for archiving purposes in the public interest, or for scientific, statistical and historical research purposes.

38 Other rights

Do individuals have other substantive rights?

Individuals have the right to require the rectification of incomplete or inaccurate data without undue delay, as well as to fill in incomplete data, if it is necessary for the processing.

Individuals have the right to ask for the erasure of personal data without undue delay, particularly if:

- the personal data is no longer necessary in relation to the purposes of processing;
- the person requesting the erasure withdraws the consent on which the processing is based and there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing or the data subject objects to processing for direct marketing; or
- the data has to be erased for compliance with a legal obligation.

Individuals have the right to request restriction of processing if the accuracy of personal data is disputed, for so long as it is needed so that the PII owner verifies the accuracy of the personal data.

Individuals have the right to receive their personal data in a structured, commonly used and machine-readable format, as well as the right to request the direct transmission of personal data to another, if this is technically feasible.

Individuals may oppose the processing of personal data that takes place without their consent.

Individuals may not be subject to fully automated individual decision making, including profiling.

If processing occurs based on consent, individuals have the right to withdraw their consent for that processing at any time in the way they gave it.

Individuals have the right to lodge a complaint with the Greek Data Protection Authority for a data law breach.

39 Compensation

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 shall be compensated for monetary damages, either actual or for injury to feelings, if they are affected by a breach of the law. Individuals may seek compensation both from the PII owner and jointly from the PII owner and the PII processor for matters lying in the sphere of their joint liability, such as those covered by the data processing agreement between them.

40 Enforcement

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

These rights are exercisable through the judicial system and by the supervisory authority, so long as the claims to exercise such rights have first been raised with the PII owner and have not been satisfied or fully satisfied.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

According to the law under preparation implementing the GDPR, the obligation to notify a data breach to the data subject may not take place if processing occurs for the purpose of national security, defence, public order, criminal investigations or criminal prosecutions, important financial interests of the state such as tax issues or the defence of legal claims, provided that a notification would jeopardise such purposes.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

The supervisory authority, ie, the Greek Data Protection Authority, is an administrative independent agency that issues enforceable administrative acts. These acts may be challenged with the judicial remedy called 'petition for annulment' before the Supreme Administrative Court, ie, the Council of State, within 60 days from their service or knowledge in any other way, and in any case in reasonable time after their issuance.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The following rules apply to the use of cookies or equivalent technology:

- the consent of the data subject has to be freely given, specific, informed, unambiguous and written. Additionally, consent must be granular;
- data processing has to be absolutely necessary to serve a legitimate cause;
- technology for data minimisation by default must be applied; and
- anonymity or pseudonymisation options must be made available to the data subject.

The provisions of the anticipated ePrivacy Regulation shall also be relevant.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Any kind of unsolicited communication for marketing purposes by electronic means is forbidden by law. Unsolicited telephone calls are possible, provided that the user has not opted not to receive such calls by enrolling in a relevant registry of the telecommunications provider. A PII owner may process the email addresses of its customers to market its own similar products or services, another legal entity even in the same group of companies thus being excluded, provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their electronic contact details both at the time of their collection and in the content of each message sent, eg, by clicking on a clearly visible 'unsubscribe' button in the message. It is noted that unsolicited marketing communications should be clearly recognisable as such and should indicate the identity of the PII owner.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

No specific rules or regulations have been issued on cloud computing services by the Greek Data Protection Authority. The Greek Data Protection Authority has pointed attention to the Opinion 05/2012 of the Article 29 Working Party Directive 95/46/EC WP 195 on cloud computing, 1 July 2012.

Vasiliki Christou **vchristou@outlook.com.gr**

1 Asklipiou Str
10679 Athens
Greece

Tel: +30 211 4096389, +30 6946094595
Fax: +30 211 4096389
www.linkedin.com/in/vasiliki-christou-882b79153

India

Stephen Mathias and Naqeeb Ahmed Kazia
Kochhar & Co

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

India does not have a dedicated law on data protection and privacy. India has also not adopted any international instruments on privacy or data protection. Specific provisions on privacy are found in the Information Technology Act 2000 (IT Act). The IT Act is based on the United Nations Model Law on Electronic Commerce adopted by the United Nations Commissions on Internal Trade law on 30 January 1997 vide resolution A/RES/51/162. A plethora of laws in areas such as banking, telecoms and the medical field prescribe obligations of confidentiality. Banking regulations deal with when financial institutions can transfer data overseas and the types of data that cannot be transferred overseas. Telecom regulations, by and large, prevent the transfer of customer information overseas. The code of conduct of medical practitioners prevents disclosure of patient information. The insurance regulations restrict transfer of claims-related data overseas.

The IT Act contains three provisions on data protection and privacy. Section 43A provides for compensation in the event one is negligent in using reasonable security practices and procedures (RSPP) in protecting sensitive personal data and information (SPDI) and this results in a wrongful gain or wrongful loss. It should be noted that this law provides only compensation, and only when a wrongful gain or loss results from the failure to observe RSPP. It can be argued that this is nothing but a codification of the law of negligence. This means that there is no negative consequence arising merely from the failure to observe RSPP. Further, RSPP is defined to mean such procedures stated by a law in force or as agreed to by the parties, and in the absence of both, the rules framed by the government. There is no statute that prescribes RSPP. This means that if parties, for example, an employer and an employee, agree on the RSPP to be adopted, the rules of the government would not apply.

In the guise of prescribing what constitutes RSPP, the government has issued somewhat basic and not very well-written privacy rules. As stated above, these rules apply only if the concerned parties have not agreed on the RSPP that would apply. These rules contain basic principles of privacy such as when SPDI can be collected, requirements of notice and consent, when SPDI can be transferred, etc.

Section 72A provides for criminal punishment if, in the course of performing a contract, a service provider discloses personal information without the consent of the person concerned or in breach of a lawful contract and he or she does so with the intention to cause, or knowing he or she is likely to cause, wrongful loss or wrongful gain.

Section 72 prescribes criminal punishment if a government official discloses records and information accessed by him or her in the course of his or her duties without the consent of the concerned person or unless permitted by other laws.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no specific data protection authority in India. The IT Act provides for an adjudicating officer to be appointed to adjudicate whether a person has contravened the IT Act or its rules where the claim of injury or damages does not exceed 50 million rupees. If the claim exceeds 50 million rupees, the adjudicating authority would be the civil court. The Secretary to the Ministry of Information Technology in each state government has been appointed as the adjudicating officer. The adjudicating officer has all powers of a civil court. These include summoning the attendance of persons and examining them on oath, requiring the discovery or production of documents and other electronic records, receiving evidence on affidavits and issuing commissions for the examination of witnesses or documents.

The police have the power to investigate offences under the IT Act such as under section 72 and section 72A.

Under specialised statutes relating to banking, telecom and in the medical field, the relevant sectoral regulator has powers.

3 Legal obligations of data protection authority

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

There is no data protection authority in India.

4 Breaches of data protection

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

Under section 43A, if a breach results in a wrongful gain or wrongful loss, the adjudicating officer can order compensation to be paid. The law does not prescribe what the maximum compensation is. Under section 72, the punishment is imprisonment of up to two years or a fine of up to 100,000 rupees, or both. Under section 72A, the punishment is imprisonment of up to three years or a fine of up to 500,000 rupees, or both. Other laws provide for penalties under those statutes for breach of confidentiality provisions.

Scope

5 Exempt sectors and institutions

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

The provisions under the IT Act apply to all sectors, though laws specific to particular sectors would apply concurrently. Section 43A relates to a body corporate and the rules issued thereunder exclude government from the meaning of body corporate. Section 72A covers all types of organisations. Section 72 relates only to a government officer.

It should be noted, as described in the answer to question 1, that under section 43A, the parties concerned can agree among themselves

on the RSPP to be adopted. If they do so, then the privacy rules passed by the Indian government would be excluded.

Since section 72 dealing with breach of confidentiality by a government officer is subject to other laws, if another law permits the disclosure of the information by a government officer, such disclosure would not be a violation of section 72.

Other sector-specific laws provide for exceptions relating to those sectors. For example, a doctor could disclose information in circumstances where there is a serious and identified risk to a specific person or community. Banking laws refer to the duty of confidentiality in the context of other laws, practices and usages customary among bankers.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Yes, the Indian Telegraph Act 1885 and the Information Technology Act 2000 permit the government to engage in surveillance based on certain criteria that is in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order or for prevention of incitement of the commission of an offence. These grounds are based on reasonable restrictions to free speech contained in the Constitution of India.

All surveillance has to be approved in writing by the Home Secretary of the central government or the relevant state government as the case may be. The Home Secretary is the most senior of bureaucrats tasked with maintaining law and order. Indian law does not require the permission of a court to engage in surveillance.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Many laws provide a duty on service providers to maintain confidentiality of customer information. For example, medical laws deal with maintaining confidentiality of patient information. Such laws, for example, relate to medical termination of pregnancy and mental health. The code of ethics for medical professionals also prescribes that doctors must maintain confidentiality of patient information.

Banking laws also deal with protection of confidentiality of customer information. This is provided both in statutes relating to banks and payment systems as well as regulations passed by India's central bank, the Reserve Bank of India (RBI), on customer servicing, credit card operations of banks, etc.

A statute dealing with credit information companies requires credit information companies and credit institutions (banks, etc) to adopt principles relating to collection of information, processing of such information, protection of data and the manner of access and sharing of data. The principles are not prescribed by the law or by the regulator but have to be framed by the concerned credit information companies and institutions.

The RBI has prescribed detailed guidelines on information security, electronic banking, technology risk management and cyber frauds. In particular, the guidelines mention that banks must report breaches to the RBI and require use of encryption technology of at least 128-bit SSL and implementation of ISO/IEC 27001 and ISO/IEC 27002. Further, the banking regulations require banks to appoint a chief information security officer who will be responsible for articulating and enforcing the policies that banks use to protect their information assets apart from coordinating security-related issues.

RBI regulations on outsourcing also deal with the ability of banks to transfer data outside India. This is permitted, provided that:

- the offshore regulator will not obstruct the arrangement or prevent inspections by the RBI or auditors;
- the availability of records to the management and RBI would withstand the liquidation of the offshore provider or the bank in India;
- the offshore regulator does not have access to the data simply because the data is being processed overseas; and
- the jurisdiction of the courts in the offshore location would not extend to the operations of the bank in India.

The outsourcing regulations also require customer data to be isolated and clearly identified, and there can be no comingling of data. Telecom laws, by and large, prohibit the transfer of customer accounting and user information outside of India except with regard to roaming information and remote access to such data from outside India. A recent notification issued by the RBI imposes restrictions on overseas transfers of payment system data by payment system operators.

8 PII formats

What forms of PII are covered by the law?

While section 72A covers personal information, section 43A covers SPDI. Personal information means information that relates to a natural person, which either directly or indirectly in combination with other information available or likely to be available with a body corporate is capable of identifying such person. SPDI covers the following:

- passwords;
- financial information such as bank account or credit card or debit card or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation; medical records and history; and
- biometric information.

The law does not distinguish personal information on the basis of the format of the information, such as electronic as opposed to physical records. However, the laws on SPDI are applicable only to SPDI in electronic form.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The law does not specify whether it applies only to PII owners or processors of PII established or operating in the jurisdiction. After the privacy rules were notified, there was some concern that they would apply to SPDI of foreign nationals that was being processed in India by the many business process outsourcing businesses in India. The government then issued a press note to clarify that it relates only to a body corporate or person located within India. Further, data processing as a result of a contract between two entities is not covered by the privacy rules. While the clarification is not entirely clear, the accepted view is that this does not apply to foreign personal information being processed in India.

The law does allow transfer of SPDI out of India only if the recipient ensures the same level of data protection.

10 Covered uses of PII

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

The law is not entirely clear on this point, though there is a clarification that appears to suggest that the privacy rules relate to a party that collects the data directly from the providers of the information and does not relate directly to a situation where the processor of the information receives the information from another body corporate. At the same time, the law allows transfer of SPDI only if the recipient ensures the same level of data protection. The two provisions are somewhat contradictory as one exempts onward transfers and the other appears to apply the rules to onward transfers.

Legitimate processing of PII

11 Legitimate processing – grounds

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

Yes, SPDI cannot be collected unless the information is collected for a lawful purpose connected with a function or activity of the party collecting or using the information and the collection of the SPDI is considered necessary for that purpose. Apart from this, there are also notice and consent requirements.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Section 43A and the privacy rules relate to SPDI, which have a narrower meaning than personal information. Personal information is referred to in section 72A. See question 1 for definitions of both SPDI and personal information.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

While collecting SPDI, the provider must be made aware through reasonable steps of the following:
- the fact that the information is being collected;
- the purpose for which it is collected;
- the intended recipients of the information; and
- the name and address of the agency collecting or retaining the information.

Consent must be obtained from the provider of the SPDI regarding purpose of usage before collection of the information. Further, of the three grounds on the basis of which disclosure of SPDI is permitted to a third party, one relates to the provider of the information agreeing to the same and another relates to it being permitted under a contract with the provider.

14 Exemption from notification

When is notice not required?

There is no exemption to providing notice. It may be noted, however, that the privacy rules may not apply where the parties have agreed on their own terms of RSPP. The privacy rules also do not appear to apply to transfer of SPDI from one entity to another as opposed to from an individual provider of his or her own information to a data processor. It should also be noted that the privacy rules do not apply to the government.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

No, the privacy rules do not offer individuals any degree of choice or control over the use of their information, although consent is required as to the purpose of the use so the individual may simply refuse to permit the use of his or her SPDI or withdraw his or her consent later. The collecting party then has the option not to provide the goods or services for which the information was sought.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The privacy rules deal with this only indirectly. As regards currency, the SPDI cannot be retained for longer than is required for the purpose for which the information can lawfully be used or is otherwise required under any other law for the time it is in force. As regards accuracy, the provider of the information has the right to review the information it provided and correct any inaccuracy. However, this appears to relate only to information provided by the individual and not information collected separately.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes, the privacy rules specify that the SPDI cannot be retained for longer than is required for the purpose for which the information can lawfully be used or is otherwise required under any other law currently in force.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes. SPDI cannot be collected unless:
- the information is collected for a lawful purpose connected with a function or activity of the party collecting or using the information;
- the collection of the SPDI is considered necessary for that purpose; and
- the information collected is used for the purpose for which it has been collected.

There is no requirement however that the purpose of use must be specific in its description.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The privacy rules do not provide for any exceptions or exclusions. The purpose of collection or usage must be mentioned in the privacy policy. Further, consent is required as to the purpose of usage. Strictly speaking, if the new purpose is not covered by the purpose for which consent was given, the SPDI cannot be used for the new purpose. Since consent is required as to the purpose of use, change in the purpose, whether through the privacy policy or otherwise, would require the consent of the provider of the information. It must be noted that the privacy rules do not require that the purpose must be described in specific terms. It would appear, therefore, that if consent is obtained for a broad purpose, this would be sufficient.

Security

20 Security obligations

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

Section 43A refers to RSPP, which is determined by a law in force (of which there is none) or as agreed to by the parties and in the absence of both, the rules framed by the government, that is, the privacy rules. Accordingly, the parties can agree on the security standards to be adopted. The privacy rules do not stipulate a particular security standard (though that was what the rules were meant to do). The privacy rules merely suggest that IS/ISO/IEC 27001 or a code prescribed by an industry association and approved by the government could be used. So far, no code has been approved by the government.

The banking regulations require banks to follow ISO/IEC 27001 and ISO/IEC 27002. Similarly, the securities exchange regulations require stock exchanges, depositories and clearing corporations to follow standards such as ISO 27001, ISO 27002, COBIT 5, etc.

21 Notification of data breach

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 two situations in which data breach notifications apply. First, banks are required to notify the central bank, that is, the Reserve Bank of India, in case of any cybersecurity incident within two to six hours.

Second, the intermediaries, as part of their due diligence requirement in order to make use of safe harbour from content liability, are required to report cybersecurity incidents to the Computer Emergency Response Team (CERT) as soon as possible. This is not a mandatory

requirement and is required only if the intermediaries intend to use the safe harbour protection from content liability.

The definition of 'intermediary' is wide and includes telecommunications companies, ISPs, network service providers, web hosts, search engines, online payment/auction sites, online marketplaces, etc.

The data breach notifications are somewhat unclear as to whether breach notifications are mandatory or not, since the actual language states that parties 'may' notify the CERT. More recently, the CERT has been taking the view that breach notifications are mandatory for all parties and not just for intermediaries.

The data breach regulations define 'cybersecurity incident' to mean any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data without authorisation. There is a further definition through a description of various incidents that constitute cybersecurity incidents. These are:

- targeted scanning or probing of critical networks and systems;
- compromise of critical systems or information;
- unauthorised access of IT systems or data;
- defacement of a website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites, etc;
- malicious code attacks such as spreading of viruses, worms, Trojans, botnets or spyware;
- attacks on servers such as database, mail and DNS, and network devices such as routers;
- identity theft, spoofing and phishing attacks;
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks; and
- attacks on applications such as e-governance, e-commerce, etc.

The Ministry of Communication and Information Technology has set up CERT under the IT Act. CERT is the nodal agency for resolving cybersecurity incidents in India. It is responsible for scanning cyberspace for cybersecurity vulnerabilities, breaches and malicious activity and can block web pages and websites.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The privacy rules provide for the need to appoint a grievance officer to address discrepancies and grievances of providers of information. There is no requirement for the appointment of a data protection officer.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

No requirements have been prescribed for maintaining internal records or establishing internal processes or documentation except the suggestion in the privacy rules that IS/ISO/IEC 27001 is one such security standard that could be adopted.

24 New processing regulations

Are there any obligations in relation to new processing operations?

There are no obligations in relation to new processing operations under the present law. A new privacy statue is under way and it may include obligations relating to new processing operations.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

No, owners and processors of PII are not required to register with the supervisory authority.

26 Formalities

What are the formalities for registration?

Not applicable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

There are no such duties imposed under the present law.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The law regulates the disclosure or transfer of the SPDI to a third party. This is possible if it has been agreed in a contract with the provider, it is necessary for compliance of a legal obligation or prior permission is given by the provider.

Further, the privacy rules prescribe that SPDI can be transferred only to a third party that observes the same level of data protection as provided by the privacy rules. Further, the privacy rules prescribe that transfer is permitted only if necessary for the performance of the contract with the provider or where the provider has consented to the transfer. At the same time, a clarification appears to suggest that some of the privacy rules apply only between the individual provider of the information and the owner of PII and not between two entities. The two provisions do not entirely read harmoniously together.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

There are no restrictions other than those stated above.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

SPDI or any information can be transferred to a person outside India if he or she ensures the same level of data protection as provided by the rules. Further, such transfer is permitted only if necessary for the performance of the contract with the provider or where the provider has consented to the transfer.

Further, Indian company law requires companies that maintain their books of accounts and books and papers in electronic form outside India to keep a backup of such books of accounts and books and papers in servers physically located in India.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, transfer of PII does not require notification to or authorisation from a supervisory authority.

36 Further transfer

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 is not entirely clear on this matter. Transfer of SPDI to a third party can be done only if it agrees to ensure the same level of protection under the privacy rules. We believe that it follows, therefore, that if transfer of PII from the owner to a service provider is subject to restrictions, the restrictions should apply to a further transfer from the service provider to another service provider. It may also be noted that notice has to be given to the provider of the information of the name and address of every agency that will have access to such information. This would, therefore, cover onward transfers.

Rights of individuals

37 Access

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

Yes, they have a right to access their personal information and also correct the same, but this appears to relate only to personal information provided by them and not personal information obtained separately.

38 Other rights

Do individuals have other substantive rights?

By and large the rights of individuals are covered in the answers to the questions in this chapter.

39 Compensation

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 law provides for compensation to be paid if the owner is negligent in using RSPP to protect the SPDI and it results in a wrongful loss or wrongful gain. The terms 'wrongful gain' and 'wrongful loss' are not defined in the IT Act but are defined under the Indian Penal Code. 'Wrongful gain' is defined to mean gain by an unlawful means of property to which the person gaining is not legally entitled. 'Wrongful loss' means loss by unlawful means of property to which the person losing it is legally entitled. While the definitions in the penal code cannot entirely be accepted under section 43A, since the purpose of the provisions are different, we believe they do have some persuasive value. In our view, given the manner in which section 43A is constructed and the meaning of 'wrongful gain' and 'wrongful loss' under Indian laws, it is more likely that actual damage would be required.

40 Enforcement

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

Compensation can be awarded by the adjudicating officer if the claim for damages does not exceed 50 million rupees. If the claim exceeds 50 million rupees, the rights would be exercisable through the judicial system.

Update and trends

Data protection has been trending for the past several months in India. The Supreme Court of India in August 2017 delivered a landmark judgment recognising the right to privacy as a fundamental right. In addition, the government of India, a few months after the decision, in its efforts to frame a separate data protection law, issued a white paper on a data protection framework for India for public comments. The last date for public comments has lapsed and the government should be able to place the draft data protection bill soon.

The Ministry of Health and Family Welfare has published the draft Digital Information Security in Healthcare Act (DISHA), inviting public comments. The DISHA lays down provisions that regulate the generation, collection, access, storage, transmission and use of digital health data and associated personally identifiable information. It seeks to enable the digital sharing of personal health records with hospitals and clinics, and between hospitals and clinics. The DISHA appears to lay the groundwork for many health exchanges. However, there shall be no access to or disclosure of personally identifiable information to any third party.

The banking regulator has imposed data localisation restrictions; payment systems processors are required to store payment data within India.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

As stated in question 20, the privacy rules come out of the power of the government to prescribe what RSPP is. RSPP is as per a law in force or as agreed between the parties and only in the absence of both would the rules of the government (that is, the privacy rules) apply. Accordingly, if the parties (eg, employer and employee or service provider and customer) agree on the RSPP, then the privacy rules would not apply. Further, through the definition of body corporate, the privacy rules do not apply to the government.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, decisions of the adjudicating officer can be appealed to the Cyber Appellate Tribunal. Decisions of the Cyber Appellate Tribunal can be appealed to the High Court.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Indian law does not deal directly with the use of cookies or equivalent technology. Indian law does provide for both compensation and criminal punishment where, without the permission of the owner or the person in charge of the computer, computer system or computer network, a person downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network. Read literally, it would appear that consent is required for the use of cookies. However, it is possible to get around this by including such usage in the terms of use. Under Indian contract law, as long as there is reasonable sufficiency of notice that certain terms apply to the use of a website and the terms are not unfair or unconscionable, these terms are likely to be enforceable against the customer or user.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Indian law does not deal with marketing through email or fax. In 2015, a badly worded provision that appeared to deal with spam was struck down by the Supreme Court of India as being unconstitutional.

The IT Act does not cover electronic marketing. This is covered by 'do not call' rules framed by the Telecom Regulatory Authority of India (TRAI). Persons can register their numbers on a Do Not Call registry. Certain exceptional categories have been provided. Persons can register to receive communications only in those categories. These categories are:

- banking, insurance, financial products and credit cards;
- real estate;
- education;
- health;
- consumer goods and automobiles;
- communication, broadcasting, entertainment and IT; and
- tourism and leisure.

Further, SMS messages can be sent if the message is transactional in nature. Transactional messages cover only prescribed areas that include information pertaining to goods or services sent by a business to its employees, agents or customers, information pertaining to a banking, securities or insurance account, information pertaining to air and rail travel schedules and reservations, information from an educational institution to parents and students, and information by e-commerce companies in relation to transactions. Regulations also allow messaging by identified social media organisations such as Facebook, Yahoo, etc. There are also limits on how many SMSs a non-telemarketer can send in a day.

Telemarketers who make marketing calls or send marketing messages are required to be registered with TRAI. They have to obtain separate telecom resources specifically for engaging in telemarketing. They also have to obtain separate telecom resources for sending transactional messages. They are required to scrub their databases with that of the Do Not Call registry regularly. The law requires the telecom service providers (Telcos) to have backend integration with the Do Not Call registry. As a consequence, if a message is sought to be sent to a person on the Do Not Call registry and the message is not transactional in nature or the message does not relate to an exception category selected by the person, the IT systems of the Telcos will automatically block the message.

Various penalties have been prescribed where telemarketers violate the regulations. Penalties for each violation start at 25,000 rupees for the first violation and go up to 250,000 rupees for the sixth violation. On the sixth violation, the telemarketer will be blacklisted and will not be permitted to use any kind of telecom resources in India.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

India does not have any rules or regulations governing the use of cloud computing services. The TRAI has recently released a consultation paper on cloud computing. The consultation paper points out several issues relating to cloud services, such as interoperability, data security, data localisation, data ownership, cross-border movement of data and taxation of cloud services. The consultation paper is presently open for public comments, and based on the public comments and discussion with the stakeholders TRAI may soon come out with regulations governing the use of cloud computing services.

KOCHHAR & CO.
ADVOCATES & LEGAL CONSULTANTS

Stephen Mathias **stephen.mathias@bgl.kochhar.com**
Naqeeb Ahmed Kazia **naqeeb.ahmed@bgl.kochhar.com**

201 Prestige Sigma
3 Vittal Mallya Road
Bangalore 560001
India

Tel: +91 80 4030 8000
Fax: +91 80 4112 4998
www.kochhar.com

Ireland

Anne-Marie Bohan
Matheson

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The data protection regime in Ireland is currently governed by the Data Protection Acts 1988 and 2003 (collectively, the DPA). The DPA transposes European Directive 95/46/EC on data protection into Irish law.

As well as conferring rights on individuals, the DPA also places obligations on those who collect and process personal data. 'Personal data' is defined as any information relating to a living individual identifiable from that data (or from a combination of that data and other information of which the data controller is in possession or is likely to come into possession).

The DPA seeks to regulate the collection, processing, keeping, use and disclosure of personal data that is processed automatically or, in certain circumstances, manually.

The DPA places responsibilities on both 'data controllers' and 'data processors'. A data controller is a person who controls the use and contents of personal data, while a data processor refers to a person who processes personal data on behalf of a data controller.

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (ePrivacy Regulations) deal with specific data protection issues relating to use of electronic communication devices, and particularly with direct marketing restrictions.

The General Data Protection Regulation (Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) (GDPR) will have direct effect in Ireland from 25 May 2018, and will largely replace the DPA. The GDPR is intended to harmonise further the data protection regimes within the EU, and will introduce a number of changes into the data protection regime, including:

- increased scope to include focus on the residence of the data subject;
- lead authority supervision;
- privacy by design and by default;
- additional focus on processers and processing arrangements;
- improved individual rights;
- mandatory breach reporting; and
- significantly increased sanctions for breach.

A preliminary draft of the proposed national legislation dealing with member state derogations and options under the GDPR was published in May 2017.

Ireland is a signatory to both the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the European Convention on Human Rights and Fundamental Freedoms. The Charter of Fundamental Rights of the European Union also has application in Ireland.

In addition, the Irish Constitution, Bunreacht na hEireann, has been held by the Irish courts to encapsulate an unenumerated right to privacy.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The DPA confers specific rights on the Office of the Data Protection Commissioner (ODPC) and explicitly states that the ODPC shall be the supervisory authority in Ireland for the purpose of the Directive.

The ODPC is responsible for ensuring that individuals' data protection rights are respected, and that those who are in control of, or who process, personal data carry out their responsibilities under the DPA. The powers of the ODPC are as follows.

Investigations
Under section 10 of the DPA, the ODPC must investigate any complaints that it receives from individuals in relation to the treatment of their personal data unless it considers them to be 'frivolous or vexatious'. The ODPC may also carry out investigations of its own accord. In practice, these usually take the form of scheduled privacy audits. However, it should be noted that the ODPC is not prevented from conducting 'dawn raid' types of audits, if it decides to do so (as to which, see note on the powers of 'authorised officers' under section 24 of the DPA, below).

Power to obtain information
Under section 12 of the DPA, the ODPC has the power to require any person to provide it with whatever information it needs to carry out its functions. In carrying out this power in practice, the ODPC usually issues the person with an information notice in writing. It is an offence to fail to comply with such an information notice (without reasonable excuse), although there is a right to appeal any requirement specified in an information notice to the Circuit Court under section 26 of the DPA.

Power to enforce compliance with the Act
Under section 10 of the DPA, the ODPC may require a data controller or data processor to take whatever steps it considers appropriate to comply with the terms of the DPA. In practice, this may involve blocking personal data from use for certain purposes, or erasing, correcting or supplementing the personal data. This power is exercised by the ODPC issuing an enforcement notice.

Power to prohibit overseas transfer of personal data
Under section 11 of the DPA, the ODPC may prohibit the transfer of personal data from Ireland to an area outside of the European Economic Area (EEA). In exercising this power, the ODPC must have regard to the need to facilitate international transfers of information.

The powers of authorised officers
Under section 24 of the DPA, the ODPC has the power to nominate an authorised officer to enter and examine the premises of a data controller or data processor, to enable the ODPC to carry out its functions.
An authorised officer has a number of powers, such as: the power to enter the premises and inspect any data equipment there; to require the data controller or data processor to assist him or her in obtaining access to personal data; and to inspect and copy any information.

Enforcement

The ODPC may bring summary legal proceedings for an offence under the DPA or the ePrivacy Regulations. The ODPC does not have the power to impose fixed monetary penalties, unlike the Information Commissioner in the UK.

The enforcement regime is likely to change significantly following the coming into force of the GDPR, not least in that it is anticipated that the ODPC will be replaced by the Data Protection Commission (Commission), which will assume the ongoing work of the ODPC. It is currently proposed that there may be up to three Data Protection Commissioners appointed to the Commission, which is likely to qualify as the lead authority for a significant number of large social media companies and other controllers of large volumes of personal data with headquarters in Ireland. In addition, for the first time the Commission will have the authority to impose administrative fines directly on controllers and processors (subject to a right of appeal to the courts).

3 Legal obligations of data protection authority

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

Please see the Getting the Deal Through website (www.gettingthedealthrough.com).

4 Breaches of data protection

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

Yes. While most of the penalties for offences under the DPA are civil in nature, breaches of data protection can also lead to criminal penalties.

Summary legal proceedings for an offence under the DPA may be brought and prosecuted by the ODPC. Under the DPA, the maximum fine on summary conviction of such an offence is set at €3,000. On conviction on indictment (such a conviction in Ireland is usually reserved for more serious crime), the maximum penalty is a fine of €100,000.

The ePrivacy Regulations specify the sanctions for breaches of electronic marketing restrictions, which on summary conviction are a fine of up to €5,000 (per communication), or on conviction on indictment to maximum fines ranging from €50,000 for a natural person to €250,000 for a body corporate.

Under the GDPR, sanctions for breach will increase substantially, and will range from up to €10 million or 2 per cent of worldwide turnover to up to €20 million or 4 per cent of worldwide turnover, depending on the breach.

Scope

5 Exempt sectors and institutions

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

The DPA applies to all sectors and all types of organisation. Some areas of activity are, however, outside the scope of the DPA. Under section 1(4) the DPA does not apply if the personal data:

- is or at any time was kept for the purposes of safeguarding Ireland's security;
- consists of information that the person keeping the personal data is required by law to make available to the public; or
- is kept by an individual for his or her personal, family or household affairs, or for solely recreational purposes.

Processing may also be exempt in certain circumstances. Processing will fall outside the scope of the GDPR if it is:

- in the course of an activity outside the scope of EU law;
- for purely personal or household activities;
- by competent authorities in connection with crime or public security; or
- by member states in connection with justice and social security (Chapter 2 Title 5 TFEU).

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Electronic marketing is addressed in the ePrivacy Regulations. The ePrivacy Regulations also prohibit the listening, tapping, storage or other interception or surveillance of communications and related traffic data without consent. Further restrictions are found in the Postal and Telecommunications Services Act 1983, the Interception of Postal Packets and Telecommunications (Regulation) Act 1993 and the Criminal Justice (Surveillance) Act 2009.

The Criminal Justice (Offences Relating to Information Systems) Bill 2016 (the Bill) is currently working its way through the legislative process in Ireland, and is designed to implement certain provisions of Directive 2013/40/EU (the Cyber-Crime Directive). The Bill will introduce a specific offence addressing intercepting and transmission of data without lawful authority, will introduce more stringent penalties and will make misuse of personal data an aggravating factor in relation to sentencing.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Any processing of personal data, including in the context of e-health records, social media and financial or credit information, must comply with the principles as set out in the DPA, as well as any requirements of sectoral regulators. The Central Bank of Ireland, which authorises and regulates financial institutions and service providers in Ireland, requires high standards of data security generally, including compliance with the DPA. The Central Bank has had an increasing focus on cybersecurity risks in recent years, and published cross-industry guidance in respect of information technology and cybersecurity risks, which includes data security guidance, in September 2016. Processing of genetic data is subject to additional restrictions in the Disability Act 2005 and the Data Protection (Processing of Genetic Data) Regulations 2007. Collection and use of personal public service numbers is also subject to restrictions.

Further data protection requirements, including in relation to phone, email, internet and SMS use in connection with unsolicited communications, are set out in the ePrivacy Regulations, which implement Directive 2002/58/EC (the ePrivacy Directive), and are of particular importance to providers of publicly available electronic communications networks and services, as well as businesses engaged in direct marketing. The European Commission has published a proposal for an ePrivacy Regulation, which if enacted would replace the Irish ePrivacy Regulations with potentially more restrictive requirements.

8 PII formats

What forms of PII are covered by the law?

Personal data includes any automated and manual data (ie, data that is recorded as part of a structured filing system) relating to a living individual who can be identified from the personal data in question (or from a combination of that data and other information of which the data controller is in possession or is likely to come into possession).

Under the GDPR, the definition of personal data will be clarified and will cover any information relating to an identified or identifiable person, with an identifiable person being one who can be identified directly or indirectly, in particular by reference to an identifier such as, for example, a name, ID number, location data, online identifier, etc.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Unitl 25 May 2018, yes. The DPA applies to data controllers in respect of the processing of personal data only if:

- the data controller is established in Ireland, and the data is processed in the context of that establishment; or
- the data controller is established neither in Ireland nor in any other state that is a contracting party to the European Economic

Area (EEA) Agreement, but makes use of equipment in Ireland for processing the data otherwise than for the purpose of transit through the territory of Ireland. Such a data controller must, without prejudice to any legal proceedings that could be commenced against the data controller, designate a representative established in Ireland.

Each of the following shall be treated as established in Ireland:
- an individual who is normally resident in Ireland;
- a body incorporated under the laws of Ireland;
- a partnership or other unincorporated association formed under the laws of Ireland; and
- a person who does not fall within any of the above, but who maintains in Ireland:
  - an office, branch or agency through which he or she carries on any activity; or
  - a regular practice.

The GDPR will extend the scope of application of EU data protection rules, focusing as it does on the location of the data subject in the EU, rather than simply the place of establishment of the data controller. The GDPR will have application to non-EU controllers who offer goods and services to individuals in the EU or who monitor the behaviour of individuals as far as the behaviour takes place in the EU.

10 Covered uses of PII

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

The DPA applies to individuals or organisations established in Ireland that collect, store or process personal data on any form of computer system and in certain forms of structured manual filing systems. There are no exclusions from scope, save as described in response to question 5.

Under the DPA, a distinction is made between those who control personal data and those who process it. A 'data controller' is one who (either alone or with others), controls the use and contents of personal data, while a 'data processor' refers to a person who processes data on behalf of a data controller. Generally, those who provide services to owners will be data processors. Employees who process personal data in the course of their employment are not included in these definitions.

Data controllers are subject to the full scope of the DPA. Data processors have fewer direct statutory obligations, but importantly are subject to the data security principle, and owe a statutory duty of care to data subjects.

The GDPR retains the distinction between data controllers and data processors, but significantly increases the focus on processing activities. Data processors will have additional obligations once the GDPR comes into force.

Legitimate processing of PII

11 Legitimate processing – grounds

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

Yes. Under section 2A(1)(a) of the DPA, consent of the individual is a legitimate ground for processing personal data. Data controllers can also process personal data (excluding sensitive personal data – see question 12) without the data subject's consent if it is necessary for one of the following reasons:
- for the performance of a contract to which the data subject is a party (including steps taken at the request of the data subject before entering into the contract);
- for compliance with a legal obligation, including:
  - the administration of justice;
  - the performance of a function conferred on a person by law;
  - the performance of a function of the government or a minister of the government; and
  - the performance of any other function of a public nature, which is performed in the public interest;
- to prevent injury or other damage to the health, or serious loss or damage to the property, of the data subject;
- to protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged; and
- for the purpose of the legitimate interests pursued by a data controller, except if processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

Section 8 of the DPA details circumstances in which the restrictions in the DPA (including consent) do not apply (eg, if the processing of personal data is required for the investigation of an offence, or by order of a court or under an enactment or rule of law).

The legitimate processing grounds in the DPA apply in addition to the data protection (or data quality) principles (see questions 13 and 16 to 20).

The legitimate processing grounds in the DPA are narrowly interpreted.

The GDPR contains broadly similar provisions, but expands on the concept of consent, imposing on the data controller a requirement to demonstrate consent has been obtained by a statement or clear affirmative action. It is expected that the legitimate processing grounds under the GDPR will also be narrowly construed.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Yes. In addition to the requirements outlined in question 11, section 2B of the DPA imposes the following additional obligations on the data controller for the processing of sensitive personal data:
- the data subject, or a parent or legal guardian (where applicable), must give explicit consent, having been informed of the purpose of the processing; and
- if consent is not obtained, a data controller can still process the sensitive personal data if the processing is necessary for:
  - exercising or performing any right or obligation that is conferred or imposed by law on the data controller in connection with employment;
  - preventing injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where consent cannot be given or the data controller cannot reasonably be expected to obtain such consent;
  - preventing injury to, or damage to the health of, another person, or serious loss in respect of, or damage to, the property of another person, in a case where such consent has been unreasonably withheld;
  - carrying out the processing for a not-for-profit organisation in respect of its members or other persons in regular contact with the organisation;
  - processing information that has already been made public as a result of steps deliberately taken by the data subject;
  - obtaining legal advice, obtaining information in connection with legal proceedings, or where processing is necessary for the purposes of establishing, exercising or defending legal rights;
  - obtaining personal data for medical purposes;
  - processing by a political party or candidate for election in the context of an election;
  - assessing or paying a tax liability; or
  - administering a social welfare scheme.

For the purposes of the DPA, sensitive personal data includes information in relation to physical or mental health, racial or ethnic origin, political opinions, religious or philosophical beliefs, the commission or alleged commission of any offence, proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings.

Under the GDPR, a broadly similar approach is taken to the processing of sensitive (recharacterised as 'special') categories of personal data. However, data relating to criminal convictions and offences will

be treated slightly differently, and may only be processed by official authorities or if authorised by law providing for appropriate safeguards for individual rights and freedoms.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Data subjects need to be notified of certain matters at the point of collection of personal data. Personal data is not considered to be processed fairly, under the data protection principles, unless, in the case of personal data obtained directly from the data subject, the data controller ensures that the data subject has been provided with at least the following information at the point of collection:

- the name of the data controller;
- the purpose for collecting the personal data;
- the identity of any representative nominated for the purposes of the DPA;
- the persons or categories of persons to whom the personal data may be disclosed;
- whether replies to questions asked are obligatory and if so, the consequences of not providing replies to those questions;
- the data subject's right of access to their personal data;
- the data subject's right to rectify their data if inaccurate or processed unfairly; and
- any other information which is necessary so that processing may be fair, and to ensure the data subject has all necessary information to be aware as to how their personal data will be processed.

Many of these points are typically dealt with in a data controller's terms and conditions or privacy policy.

Where information is indirectly obtained, the data subject must also be informed of the categories of data and the name of the original data controller.

The GDPR places greater emphasis on transparency, and will require more specific disclosures to data subjects, in intelligible and clearly accessible form, using clear and plain language.

14 Exemption from notification

When is notice not required?

There is an exemption from notification where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of the information specified therein proves impossible or would involve a disproportionate effort, or in any case where the processing of the information contained or to be contained in the personal data by the data controller is necessary for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract.

Under the GDPR, the notice requirements will apply unless the data subject already has the information, or in the case of indirectly obtained personal data, the provision of the information would be impossible or involve disproportionate effort, the obtaining and disclosure of the personal data is expressly set out in law, or the personal data is subject to an obligation of professional secrecy.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Yes. An individual can have his or her personal data rectified, blocked or deleted if he or she requests this in writing. The relevant information must be provided as soon as possible following a data subject access request, and no later than 40 days following compliance with section 4 of the DPA by the individual requesting the information.

In addition, an individual has the right to object to processing that is likely to cause damage or distress. This right applies to processing that is necessary for either:

- the performance of a task carried out in the public interest or in the exercise of official authority; or
- the purposes of the legitimate interests pursued by the data controller to whom the personal data is, or will be, disclosed, unless those interests are overridden by the interests of the data subject in relation to fundamental rights and freedoms and, in particular, his or her right to privacy.

Objections to current or future processing can be submitted in writing to the data controller.

Furthermore, unless a data subject consents, a decision that has a legal or other significant effect on him or her cannot be based solely on the processing by automatic means of his or her personal data, which is intended to evaluate certain personal matters relating to him or her (for example, his or her performance at work, creditworthiness, reliability and conduct).

Individuals also have the right to control the extent to which they receive marketing (including, in particular, by electronic means), and to be removed from marketing databases.

Under the GDPR, in addition to the rights of access, rectification, erasure (ie the right to be forgotten) and restriction of processing, data subjects will in certain circumstances have the right to object to processing and to data portability. None of the rights under the GDPR is an absolute right, and each may be made subject to certain restrictions.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Yes. Data controllers must keep the personal data safe and secure, accurate, complete and, where necessary, up to date.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes. Data controllers must ensure that personal data is adequate, relevant and not excessive and retain it for no longer than is necessary for the specified purpose or purposes for which it was obtained.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes. The DPA specifies that data controllers must obtain personal data only for specified, explicit and legitimate purposes, and process the personal data only in ways compatible with the purposes for which it was obtained by the data controller initially.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The finality principle does not apply to personal data kept for statistical, research or other scientific purposes, and the keeping of which complies with such requirements as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects if the personal data is not used in such a way that damage or distress is caused to any data subject.

Section 8 of the DPA details circumstances in which the restrictions in the DPA (including the finality principle) do not apply. This includes where the data subject has requested or consented to the new purpose.

Under the GDPR, processing for purposes other than those for which the personal data was originally collected should only be allowed where the further processing is compatible with the original purposes.

Security

20 Security obligations

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

According to section 2 of the DPA, data controllers must have 'appropriate security measures' in place. Data processors are subject to the same data security principle, which must also be included in processing

contracts. These measures adopted must be appropriate to the nature of the data concerned and must provide a level of security that is appropriate to the potential level of harm that could result from any unauthorised or unlawful processing or from any loss or destruction of personal data. Data controllers and data processors must also ensure that their employees comply with any and all security measures in place.

The GDPR adopts a 'privacy by design and by default' approach to data protection, putting security at the core of data protection obligations, and will impose on the data controller the need to demonstrate compliance with the GDPR. Both data controllers and data processors will be subject under the GDPR to obligations relating to the security of personal data.

21 Notification of data breach

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 ODPC has published the 'Personal Data Security Breach Code of Practice' (the Code), which contains specific data security breach guidelines. This Code is non-binding in nature and does not apply to providers of publicly available electronic communications services in public communications networks in Ireland, which are subject to a mandatory reporting obligation under the ePrivacy Regulations.

The following guidelines are provided for in the Code:

- when a data breach occurs the data controller should immediately consider whether to inform those who will be or have been impacted by the breach;
- if a breach is caused by a data processor he or she should report it to the data controller as soon as he or she becomes aware of it;
- if the personal data was protected by technological measures (such as encryption) to such an extent that it would be unintelligible to any person who is not authorised to access it, then the data controller may decide that there is no risk to the personal data (and so no notification to the data subject necessary);
- any incident which has put personal data at risk should be reported to the ODPC as soon as the data controller becomes aware of it. There are some limited exceptions to this provided for in the Code; for example, this is not required where:
  - it affects fewer than 100 data subjects;
  - the full facts of the incident have been reported without delay to those affected; and
  - the breach does not involve sensitive personal data or personal data of a financial nature; and
- if the data controller is unclear about whether or not to report the incident, the Code advises that the incident should be reported to the ODPC. The Code advises that the controller should make contact with the ODPC within two working days of becoming aware of the incident.

Once the ODPC is made aware of the circumstances surrounding a breach or a possible breach, it will decide whether a detailed report or an investigation (or both) is required.

Breach notification will become mandatory once the GDPR comes into effect. Controllers will be obliged to notify the Commission where there has been a breach unless the breach is unlikely to result in a risk to data subjects. Data subjects must be informed of a breach without undue delay where the breach is likely to result in a high risk to them.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

No. While the DPA does not provide specifically for the appointment of a data protection officer, when registering with the ODPC, both data controllers and data processors must give details of a 'compliance person' who will supervise the application of the DPA within the organisation in relation to personal data that is collected.

Under the GDPR, it will be compulsory to appoint a data protection officer in certain circumstances (for example, public authorities and bodies must appoint them, as well as organisations whose core activities consist of the systematic monitoring of data subjects on a large scale or the large-scale processing of special categories of personal data).

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

No specific rules relating to internal records are provided for in the DPA. This will change once the GDPR comes into effect. The GDPR will increase focus on processors and processing, and will mandate records of processing activities.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Please see the Getting the Deal Through website (www.gettingthedealthrough.com).

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

Yes. The specific requirements relating to registration are dealt with under sections 16 to 20 of the DPA and secondary legislation.

It is mandatory for certain types of data processors and data controllers to register with the ODPC if they hold personal data in automated form and have a legal presence in Ireland, or use equipment located here.

It is obligatory for the following parties to register with the ODPC and no exemption may be claimed on their behalf:

- government bodies or public authorities;
- banks, financial or credit institutions and insurance undertakings;
- data controllers whose business consists wholly or mainly of direct marketing;
- data controllers whose business consists wholly or mainly in providing credit references;
- data controllers whose business consists wholly or mainly in collecting debts;
- internet access providers, telecommunications networks or service providers;
- data controllers that process genetic data (as specifically defined in section 41 of the Disability Act 2005);
- health professionals processing personal data related to mental or physical health; and
- data processors that process personal data on behalf of a data controller in any of the categories listed above.

Exemptions

Generally, all data controllers and processors must register unless an exemption applies, either under section 16(1)(a) or (b) or under SI No. 657 of 2007. Under section 16(1)(a) or (b) the following are excluded from registration:

- organisations that only carry out processing to keep, in accordance with law, a register that is intended to provide information to the public;
- organisations that only process manual data (unless the personal data had been prescribed by the ODPC as requiring registration); and
- organisations that are not established or conducted for profit and that are processing personal data related to their members and supporters and their activities.

Additionally, pursuant to SI No. 657 of 2007, the Irish Minister for Justice and Equality has specified that the following data controllers and data processors are not required to register (provided they do not fall within any of the categories in respect of which no exemption may be claimed):

- data controllers who only process employee data in the ordinary course of personnel administration and where the personal data is not processed other than where it is necessary to carry out such processing;

- solicitors and barristers;
- candidates for political office and elected representatives;
- schools, colleges, universities and similar educational institutions;
- data controllers (other than health professionals who process data relating to the physical or mental health of a data subject for medical purposes) who process personal data relating to past, existing or prospective customers or suppliers for the purposes of:
  - advertising or marketing the data controller's business, activity, goods or services;
  - keeping accounts relating to any business or other activity carried on by the data controller;
  - deciding whether to accept any person as a customer or supplier;
  - keeping records of purchases, sales or other transactions for the purpose of ensuring that requisite payments and deliveries are made or services provided by or to the data controller in respect of those transactions;
  - making financial or management forecasts to assist in the conduct of business or other activity carried on by the data controller; or
  - performing a contract with the data subject where the personal data is not processed other than where it is necessary to carry out such processing for any of the purposes set out above;
- companies who process personal data relating to past or existing shareholders, directors or other officers of a company for the purpose of compliance with the Companies Act 2014;
- data controllers who process personal data with a view to the publication of journalistic, literary or artistic material; and
- data controllers or data processors who operate under a data protection code of practice.

If an exemption does apply, however, it is limited only to the extent to which personal data is processed within the scope of that exemption.

The ODPC is obliged not to accept an application for registration from a data controller who keeps 'sensitive personal data' unless the ODPC is of the opinion that appropriate safeguards for the protection of the privacy of the data subjects concerned are being, and will continue to be, provided by the controller.

Where the ODPC refuses an application for registration, it must notify the applicant in writing and specify the reasons for the refusal. An appeal against such decision can be made to the Circuit Court.

The registration process will no longer apply once the GDPR comes into effect.

26 Formalities

What are the formalities for registration?

Under section 17 of the DPA, an application for registration as a data processor or data controller must be filed with the ODPC. An application to register as a data controller or data processor with the ODPC can be made using an online system through the ODPC's website. Alternatively, an application form can be downloaded from the website and sent via postal service.

Fees

A fee is also required and can be paid online or by cheque. The fee for registration varies significantly depending on the number of employees (there is also some variance between postal application fees and online application fees).

For applicants with 26 employees or more (inclusive), the online application fee is €430, while the postal application fee is €480.

For applicants with between six and 25 employees (inclusive), the online application fee is €90 and the postal application fee is €100.

Finally, for applicants with between zero and five employees (inclusive), the online application fee is €35, while the postal application fee is €40.

According to section 17(1)(a) it is for the ODPC to prescribe the information he or she requires for registration.

The DPA also provides that, where a data controller intends to keep personal data for two or more related purposes, he or she is only required to make one application in respect of those purposes. If, on the other hand, he or she intends to keep personal data for two or more unrelated purposes, then he or she will be required to make separate applications in respect of each of those purposes and entries will be made in the register in accordance with each such application.

Information to be included

There are separate registration forms available on the ODPC's website for the registration of either a data processor or a data controller. A data controller must provide a general statement of the nature of their business, trade or profession and of any additional purposes for which they keep personal data. Each application of personal data relating to the purposes that the controller lists along with the types of personal data (such as name, email, date of birth) must also be listed or described. For each of these applications listed, a list of the persons or bodies to whom the personal data may be disclosed must also be given.

If any transfers are made (or intended to be made) to a country outside of the EU member states, a list of these countries along with a description of the data to be transferred and the purpose of the transfer must be provided.

Information on any sensitive personal data that is kept by the controller must also be given (such as data relating to race, religion, sex life, criminal convictions).

For data processors, a name, address and details on the nature of the data being processed must also be provided.

Finally, for both processors and controllers details of a 'compliance person' who will supervise the application of the DPA within the organisation in relation to personal data that are collected must be given.

Validity and renewal

The registration is valid for one year (from the date the ODPC receives a correctly completed application form and fee). Unless renewed after a period of one year, the entry on the register will expire. A letter is sent as a reminder approximately three weeks prior to the renewal date. Amendments may be made upon renewal free of charge. However, there is a fee for amendments made during the year-long period.

The registration process will no longer apply once the GDPR comes into effect.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Once registered, the applicant must keep their registry entry up to date. In addition, the ODPC must be informed if any part of the entry becomes incomplete or inaccurate as processing personal data without an accurate and complete entry on the register can incur a criminal penalty. It is an offence for a data controller or data processor who is required to be registered but is not registered, to process personal data.

Under section 19(1) of the DPA, a data controller to whom section 16 applies is not permitted to keep personal data unless there is an entry on the register in respect of him or her.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Under section 17(2) of the DPA, the ODPC may refuse an application for registration by means of a Registration Refusal Notice if he or she is of the opinion that the particulars proposed for inclusion in an entry in the Register are insufficient or any other information required by him or her either has not been furnished or is insufficient, or the person applying for registration is likely to contravene any of the provisions of the DPA.

Under section 17(3) the ODPC may not accept an application for registration from a data controller who keeps sensitive personal data unless he or she is of the opinion that appropriate safeguards for the protection of the privacy of the data subjects are being, and will continue to be, provided by him or her.

29 Public access

Is the register publicly available? How can it be accessed?

Yes, under section 16 of the DPA the register is available to the public for inspection and can be accessed via a link on the ODPC's website. According to section 16 of the DPA, a member of the public may inspect the register free of charge at all reasonable times and may take copies of

or extracts from entries in the register. Upon payment of a fee, a member of the public may also obtain from the ODPC a certified copy or extract from an entry in the register (section 16(3)).

30 Effect of registration

Does an entry on the register have any specific legal effect?

Yes. Section 19 of the DPA covers the 'effect of registration' and may be summarised as follows.

A data controller to whom section 16 of the DPA applies shall not keep personal data unless there is for the time being an entry in the register in respect of him or her. A data controller in respect of whom there is an entry in the register shall not:

- keep personal data of any description other than that specified in the entry;
- keep or use personal data for a purpose other than the purpose or purposes described in the entry;
- if the source from which such personal data (and any information intended for inclusion in such personal data) are obtained is required to be described in the entry, obtain such personal data or information from a source that is not so described;
- disclose such personal data to a person who is not described in the entry (other than a person to whom a disclosure of such data may be made in the circumstances specified in section 8 of the DPA); or
- directly or indirectly transfer such personal data to a place outside Ireland other than one named or described in the entry.

31 Other transparency duties

Are there any other public transparency duties?

Please see the Getting the Deal Through website (www.gettingthedealthrough.com).

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the DPA, where a third party processes personal data on behalf of the data controller, the data controller must ensure that any and all of the processing that is carried out by the processor is subject to a contract between the controller and the processor. The contract must, among other things, contain the security conditions attached to the processing of personal data, and should also specify whether the personal data is to be deleted or returned upon termination of the contract.

The data processor must make sure that no unauthorised person has access to the personal data and that it is secure from loss, damage or theft.

The requirements applicable to data processors and the mandatory contractual provisions to be included in processing contracts will increase under the GDPR.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Under the DPA, data controllers must prevent unauthorised access to or disclosure of the personal data. Security measures should be in place to ensure the above requirements are met. The approach under the GDPR is substantially the same.

The ePrivacy Regulations set out security measures for electronically stored data applicable to providers of publicly available electronic communications networks and services.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Yes. The general rule in Ireland is that personal data cannot be transferred to third countries unless the country ensures an adequate level of data protection.

Generally transfers of personal data from Ireland to other EEA member states are permitted without the need for further approval. The transfer of personal data to a country outside the EEA, however, is prohibited, unless that country ensures an adequate level of protection for the privacy and rights of data subjects.

The ODPC can prevent transfers of personal data to other countries where it considers that the data protection rules are likely to be contravened. The ODPC does this by issuing a 'prohibition notice' to the data controller or data processor in question, which prevents any transfer outside of Ireland.

Certain countries are subject to the European Commission's findings of adequacy in relation to their data protection laws (for certain types of personal data and subject to the fulfilment of some preconditions). These countries are: Canada, Israel, Switzerland, Uruguay, the Isle of Man, Argentina, Guernsey, the Faroe Islands, Andorra and New Zealand.

If the country to which a data controller or data processor wishes to transfer is not on the approved lists above then transfer may nonetheless be possible in the following circumstances:

- where the ODPC authorises such (see following question);
- where the data subject has given clear consent to such;
- where the transfer is required or authorised by law;
- if the transfer is necessary for performing contractual obligations between the data controller and the data subject;
- if the transfer is necessary for the purpose of obtaining legal advice;
- to prevent injury or damage to a data subject's health;
- for reasons of substantial public interest; and
- to prevent serious loss to the property of the data subject.

In practice these criteria are very narrowly construed.

Other methods of enabling the transfer of personal data include using binding corporate rules (BCR), which are intra-group rules designed to allow multinational companies to transfer personal data from the EEA to affiliates located outside the EEA in compliance with Directive 95/46/EC. The BCRs are submitted to the ODPC for approval. The EU standard contractual clauses (SCCs) may also be used. These are clauses that the European Commission has approved as providing an adequate level of protection for transferred data. Approval of a data transfer agreement using the SCCs does not require approval of the ODPC. The ODPC also has the power to approve contractual clauses that do not necessarily conform to the SCCs, but in practice is only likely do so where there is a strong justification for not using the SCCs.

From 1 August 2016, US companies have been able to self-certify under the new EU-US Privacy Shield, which replaces the previous Safe Harbor regime.

Equivalent transfer restrictions and exemptions will apply under the GDPR, which helpfully anticipates processor-to-processor SCCs, and also expressly recognises BCRs.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Transfer of personal data involving a transfer to another jurisdiction, and the basis upon which the transfer is being justified, must be notified if a controller is required to register with the ODPC.

The ODPC can prohibit transfers of personal data to places outside Ireland where it considers that the data protection rules are likely to be contravened and that individuals are likely to suffer damage or distress.

36 Further transfer

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 same restrictions apply equally to transfers to service providers and onwards transfers, whether by service providers or data owners.

Rights of individuals

37 Access

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

Yes. Under section 3 of the DPA, individuals have the right to find out free of charge whether an organisation or an individual holds information

about them. This right includes the right to be given a description of the information and to be told the purposes for which that information is held. A request for this information must be made in writing by the individual and the individual must receive a reply within 21 days according to the DPA.

Section 4 of the DPA provides that individuals have the right to obtain a copy of any information that relates to them that is held either on a computer or in a structured manual filing system, or that is intended for such a system. A maximum fee of €6.35 is permitted when a request is made under section 4 and the organisation or entity is given 40 days to reply to such a request.

Exceptions to the right of access

The DPA set out specific circumstances when an individual's right of access to their personal information held by a controller may be restricted.

Disclosure is not mandatory if the information would be likely to:

- hinder the purposes of anti-fraud functions;
- damage international relations;
- impair the security or order in a prison or detention facility;
- hinder the assessment or collection of any taxes or duties; or
- to cause prejudice to the interests of the data controller where the data relates to estimates of damages or compensation regarding a claim against the data controller.

Certain information is also exempt from disclosure if the information is:

- protected by legal privilege;
- used for historical, statistical or research purposes, where the information is not disclosed to anyone else, and where the results of such work are not made available in a form that identifies any of the individuals involved;
- an opinion given in confidence; or
- used to prevent, detect or investigate offences, or will be used in the apprehension or prosecution of offenders.

If a request would be either disproportionately difficult or impossible to process the data controller or processer does not have to fulfil the request.

Exemptions also apply in respect of access to social work data, disclosure of which may be refused if it is likely to cause serious damage to the physical, mental or emotional condition of the data subject.

A request for health data may also be refused if disclosure of the information is likely to seriously damage to the physical or mental health of the data subject.

The GDPR will reduce the timeline for compliance with data access requests to one month in most cases. Such requests will also have to be complied with free of charge unless the request is manifestly unfounded or excessive.

38 Other rights

Do individuals have other substantive rights?

Yes. An individual may object to processing that is likely to cause damage or distress. This right applies to processing that is necessary for the purposes of legitimate interests pursued by the data controller to whom the personal data is, or will be, disclosed or processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

An individual has the right to have his or her data either deleted or rectified provided a request for such is made in writing (eg, a data subject can require the rectification of incorrectly held information about him or her). The person to whom the request is made must respond within a reasonable amount of time and no later than 40 days after the request. It should be noted, however, that there is no express right of an individual to request the deletion of their information if it is being processed fairly within the terms of the DPA.

Data controllers must delete personal data once it is no longer reasonably required.

As a result of the Google Spain case in 2014, data subjects may have a 'right to be forgotten' in certain circumstances.

The GDPR expands and strengthens data subject rights, introducing additional rights, such as the right to be forgotten and data portability, on a legislative basis.

The GDPR also recasts the data protection principles, reframes security obligations in a structure of data protection by design and by default, and introduces the principle of data controller accountability for compliance. Obligations as to accuracy, retention, finality and security (see questions 13 and 16 to 20) will all be impacted by these changes.

39 Compensation

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?

Where the ODPC upholds or partially upholds a complaint against an organisation for the mishandling of personal data, this does not give the complainant a right to compensation. If, however, an individual suffers damage through the mishandling of his or her personal information, then he or she may be entitled to claim compensation separately through the courts. Section 7 of the DPA makes it clear that organisations that hold personal data owe a duty of care to those individuals. Actual damage is required.

Under the GDPR, the rights of individuals to compensation for breach of their rights is clarified, and will apply whether the damage is material or non-material.

40 Enforcement

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

In the first instance, these rights are enforced by the ODPC through the courts. However, certain actions by data processors or controllers can attract either civil or criminal liability. This will continue to be the case under the GDPR, although under the GDPR, the Commission will have the power to impose administrative fines directly.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No. All exemptions and restrictions are dealt with in the answers to other questions.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes. Decisions and orders of the ODPC are appealable though the courts system. For example, if a data controller or data processor objects to a prohibition notice issued by the ODPC (such a notice prohibits transfers of personal data outside of the jurisdiction), then they have the right to appeal it to the Irish Circuit Court.

Also, an 'information notice' from the ODPC can be appealed to the Circuit Court (see question 2).

Under the GDPR, data controllers, data processors and data subjects will continue to have the right to appeal decisions of the Commission.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Under the ePrivacy Regulations the storage of cookies or of equivalent devices without the express (and informed) consent from the data subject is prohibited. Obtaining unauthorised access to any personal data through an electronic communications network is also prohibited.

There are situations, however, where the use of cookies without the express and informed consent of the data subject is allowed. This is permitted when the use of cookies is strictly necessary to facilitate a transaction, (and that transaction has been specifically requested by

the data subject). In this situation, the use of cookies is only permitted while the session is live.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Under the ePrivacy Regulations, using publicly available communications services to make any unsolicited calls or send unsolicited emails for the purpose of direct marketing, is restricted. The rules relating to such are summarised below.

Direct marketing by fax
A fax may not be used for direct marketing purposes with an individual who is not a customer, unless the individual in question has previously consented to receiving marketing communications by fax.

Direct marketing by phone
In order to contact an individual by phone for the purposes of direct marketing, the individual must:

- have given his or her consent to receiving direct marketing calls (or to the receipt of communications to his or her mobile phone as the case may be); and
- be a current customer of the company.

Direct marketing by email or text message
To validly use these methods to direct market to an individual, the individual concerned must have consented to the receipt of direct marketing communications via these methods.

An exception is where the person is firstly an existing customer and secondly the service or product that is being marketed is either the same or very similar to the product previously sold to that person.

In general, the details obtained during the sale of a product or a service can only be used for direct marketing by email if:

- the product or service being marketed is similar to that which was initially sold to the customer (ie, at the time when their details were first obtained);
- at the point when the personal data was initially collected, the customer was given the opportunity to object to the use of his or her personal data for marketing purposes (note that the manner of doing so must be free of charge and simple);
- each time the customer is sent a marketing message, he or she is given the option to opt out of such messages in the future; or
- the related sale occurred in the past 12 months, or where applicable, the contact details were used for sending an electronic marketing communication during that 12-month period.

The European Commission has published a proposal for an ePrivacy Regulation, which if enacted would replace the Irish ePrivacy Regulations with potentially more restrictive requirements.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

The ODPC has published guidance on its website relating to cloud computing services. That guidance focuses on security, data location and the requirement for a written contract that meets the requirements of the DPA. The ODPC guidance also cross refers to the 'Adopting the Cloud – Decision Support for Cloud Computing' (April 2012) published by the National Standards Authority of Ireland in conjunction with the Irish Internet Association, which provides information on the different models of cloud computing and the issues (including data protection and security) that need to be addressed by any organisation considering using a cloud provider. The ODPC guidance also references extensive guidance provided by the European Network and Information Security Agency.

** The information in this chapter is accurate as of July 2017.*

Matheson

Anne-Marie Bohan **anne-marie.bohan@matheson.com**

70 Sir John Rogerson's Quay
Dublin 2
Ireland

Tel: +353 1 232 2000
Fax: +353 1 232 3333
www.matheson.com

Italy

Rocco Panetta and Federico Sartore

Panetta & Associati

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

From 25 May 2018, the Regulation (EU) 679/2016 (the General Data Protection Regulation, or GDPR) has come into force all over Europe. However, a number of provisions require member states to legislate autonomously in order to regulate 'open' clauses of the GDPR, providing all the relevant elements of 'localisation'. This activity in Italy is currently ongoing; parliament has delegated the government to legislate and the act of implementation will consist of a legislative decree. While the first drafts of the decree have been shared, the final text is not currently available. For this reason, the answers provided in this chapter will take into consideration the letter of the GDPR and the principles of the Legislative Decree No. 196 of 2003, known as the Italian Personal Data Protection Code (the Code), the means of implementation (inter alia) of the EU Data Protection Directive No. 95/46/EC (the DP Directive) on personal data processing. Finally, in the context of this work, the terms PII and 'personal data' are used as synonyms.

The provisions of the GDPR ensure that personal data is processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection. The processing of personal data shall be regulated by affording a high level of protection for the rights and freedoms of individuals, in line and compliance with the principles of simplification, harmonisation and effectiveness of the protection granted to data subjects.

According to article 5 of the GDPR, processing of personal data shall be carried out complying with the principles of fairness, purpose, minimisation, proportionality and accountability.

Fairness
Personal data in any case shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. In particular, principles of fair and transparent processing require that the data subject shall be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data is processed.

Minimisation
Information systems and software shall be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively.

Purpose
Personal data undergoing processing shall be collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes.

Proportionality
Personal data undergoing processing shall be relevant, complete and not excessive in relation to the purposes for which it is collected or subsequently processed.

Moreover, personal data undergoing processing shall also be processed lawfully and fairly; accurate and, when necessary, kept up to date; and kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data was collected or subsequently processed. Consequently, any personal data that is processed in breach of the relevant provisions concerning the processing of personal data may not be used.

Accountability
Under the GDPR, accountability is a principle that requires organisations to put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The authority responsible for overseeing Italian data protection law is the Italian Personal Data Protection Authority (IDPA). The Authority shall act fully autonomously and independently in its decisions and assessments.

The IDPA's tasks and powers generally consist of:

- verifying whether data processing operations are carried out in compliance with laws and regulations in force;
- receiving reports and complaints, and taking steps as appropriate with regard to complaints lodged by other data subjects or associations representing their interests;
- ordering data controllers or processors to adopt such measures as are necessary or appropriate for the processing to comply with the provisions in force;
- prohibiting or blocking, in whole or in part, unlawful or unfair data processing operations;
- drawing the attention of legislators and government to the advisability of legislation as required by the need to protect the rights; and
- preferring information on facts or circumstances amounting to offences to be prosecuted, which it has come to know either in discharging or on account of its duties.

In discharging its tasks, the IDPA may request the data controller, the data processor, the data subject or a third party to provide information and produce documents.

The IDPA may order that data banks and filing systems be accessed and on-the-spot audits be performed as regards premises where the processing takes place or investigations are to be carried out with a view to checking compliance with personal data protection regulations.

The IDPA may also avail itself, if necessary, of the cooperation of other state agencies.

The inquiries, if carried out at a person's residence or in another private dwelling place or the relevant appurtenances, shall be carried out with the data controller's or data processor's informed consent. Alternatively, an authorisation from the judge presiding over the geographically competent court shall be required, whereby the judge shall issue a reasoned decree without undue delay and in any case no later than three days after receiving the relevant request from the IDPA if it can be proven that the inquiries cannot be postponed.

3 Legal obligations of data protection authority

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

Pursuant to article 60 of the GDPR, where the DPA acts as lead authority with the meaning provided in article 56 of the GDPR, the lead DPA shall cooperate with the other DPAs concerned in an endeavour to reach consensus. In this case, the lead DPA and the DPAs concerned shall exchange all relevant information with each other. Moreover, the lead DPA may request at any time other DPAs to provide mutual assistance and may conduct joint operations, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another member state.

Mutual assistance

DPAs are supposed to provide each other with relevant information and mutual assistance in order to assure uniformity of approach in the different member states. In particular, DPAs shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

Joint operations

Where appropriate (this parameter may be controversial), DPAs shall conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other member states are involved.

Furthermore, the GDPR has established a 'consistency mechanism' aimed at contributing to the consistent application of the GDPR throughout the EU. In particular, when a DPA intends to issue a decision regarding a list of topics set by the GDPR in article 64, the DPA shall communicate the draft decision to the European Data Protection Board and the Board shall issue an opinion on the matter submitted.

4 Breaches of data protection

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

Yes. According to the GDPR, breaches of data protection lead to administrative sanctions leaving to member states the chance to impose criminal sanctions. The Code currently provides criminal sanctions for the violation of data protection provisions (the implementation decree should maintain them).

Currently, from section 167 to section 172 of the Code, the Italian legislator expressly provides for criminal penalties in cases of:

- unlawful data processing (where breaches concern, for example, information notice, consent, sensitive data, traffic data, location data, unsolicited communications and so on);
- untrue declarations and notifications submitted to the IDPA;
- failure to comply with the security measures set out by the Code;
- failure to comply with provisions issued by the IDPA; and
- other mandatory obligations referring to employees' personal data protection.

Moreover, the Code expressly establishes that being convicted of any of the offences referred to in the Code shall always entail publication of the relevant judgment.

With regard to administrative sanctions, the GDPR sets forth two tiers of penalties for different conducts of non-compliance.

In particular, the first tier of conducts is sanctioned with administrative fines up to €10,000,000 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. These conducts in particular regard the violation of:

- specific obligations of the controller and the processor (eg, privacy by design principle, data processors' appointment, security measures, data protection impact assessment, etc);
- the obligations of the certification body; and
- the obligations of the monitoring body.

The second tier of conducts is sanctioned with administrative fines up to €10,000,000 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. These conducts in particular regard the violation of:

- the basic principles for processing, including conditions for consent;
- the data subjects' rights; and
- the transfer of personal data to a recipient in a third country.

The parameters for imposing administrative fines are set as a list by article 83(2) of the GDPR.

Scope

5 Exempt sectors and institutions

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

Provided the general assumption set in question 1, the GPDR sets a list of limitations at article 23 (eg, national and public security, defence, protection of judicial proceedings and independence). However, the limitations have to be implemented by the member states.

Therefore, at the moment, the Code provides that, in certain cases, specific rules apply to certain sectors and organisations. These rules in particular apply to public bodies, state defence and security matters, healthcare professionals and public healthcare bodies and so on.

The Code expressly provides for certain specific exemptions from data protection general requirements, with particular regard to processing operations carried out by the police, as well as state defence and security matters.

Information obligations are in particular excluded when processing operations are carried out in connection to state security, defence or in any way related to the prevention, suppression or detection of criminal offences. Moreover, specific exemptions are provided by section 53 in cases of processing of personal data that is directly related to the discharge of police tasks for the prevention of criminal offences, the protection of public order and public security. In this scenario, all the main data protection provisions (sections 9, 10, 12, 13, 16, 18–22, 37, 38.1–38.5 and 39–45) do not apply.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The interception of communications is considered by the Italian legislator as a very sensitive matter and it is regulated by specific rules and consistent safeguards provided for by the Italian Criminal Code and the Constitution. From a privacy point of view, the IDPA pays much attention to such matters in order to maintain an elevated level of protection for each individual who may be subject to the interception of communications. In recent years, the IDPA has issued a number of resolutions and communications to the public prosecutor's office, prescribing the necessary security measures to be complied with during interception operations. Similarly, with regard to criminal proceedings, the Code contains annex 6, regarding the rules applying to the processing of personal data performed with a view to defence investigations (the Code of the Defence Investigations). These provisions must be complied with by both lawyers and entities carrying out private investigation activities processing personal data. The purpose of the processing activities shall be carrying out defence investigations or defending a judicial claim whether during a proceeding – including administrative, arbitration and conciliation proceedings – or in the preparatory phase prior to

instituting a proceeding, or else upon conclusion of a proceeding (see section 1 of the Code of the Defence Investigations).

Finally, in June 2017 a reform of the criminal procedure code was approved by the Italian parliament, introducing new informatics tools for the interception of communications; in particular, the 'Trojans' that may be used by the prosecutor in their investigative activities.

Electronic marketing

The Code also covers electronic marketing, by providing for a specific and mandatory set of rules that each data controller has to comply with in order to lawfully process personal data for marketing purposes (see section 130 of the Code). In this regard, electronic marketing is regulated using an opt-in regime (ie, data controllers have to acquire data subjects' previous consent to lawfully process their personal data for marketing purposes, by using electronic means). Moreover, the IDPA has also issued some important measures and general resolutions to be taken into consideration, such as the resolutions concerning the guidelines on promotional activities and spam, issued by the IDPA on 4 July 2013, and the guidelines on the activities of online profiling, issued by the IDPA on 19 March 2015.

Monitoring and surveillance of individuals

The Code provides for certain general principles about the monitoring and surveillance of individuals. In particular, Law No. 300/1970 (the Statute of Workers), as well as certain general measures and guidelines issued by the IDPA, expressly establish mandatory obligations for the monitoring and surveillance of individuals.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Generally speaking, apart from the Code (and, in future, from the legislative decree of implementation), there are no further specific laws or statutes regulating different data protection areas. However, within the Italian privacy regulatory framework, a number of laws should be taken into consideration. In fact, these acts deal with relevant matters under a data protection point of view and, at the same time, contain relevant data protection provisions, as well as cross-references to the Code:

- the Statute of Workers establishes several safeguards for the processing of employees' data;
- Law No. 633/1941 provides for specific rules with regard to copyright;
- Legislative Decree No. 81/2008 provides for specific rules regarding both health and security in the workplace;
- Legislative Decree No. 206/2005 (the Consumers' Code) provides for specific rules regarding consumer protection; and
- Legislative Decree No. 70/2003 (the e-Commerce Law) establishes mandatory rules directly applicable in the e-commerce field.

Furthermore, the IDPA is always committed to issuing appropriate measures on privacy and personal data protection matters. In this regard, many focus areas are directly regulated by the IDPA's general measures, such as video surveillance, biometric data, health data, data breach notification, bank and credit information, e-health records, data processing carried out by system administrators, data processing for marketing and profiling purposes, mobile payment, cookies and so on. Finally, the Italian Criminal Code also provides data protection rules for related areas in articles 615-ter, 615-quarter and 615-quinquies of the Criminal Code, with reference to the unauthorised access to computer or telematics systems, the unauthorised detention and dissemination of access codes to computer or telematics systems, and the dissemination of tools or computer programs aimed at damaging or suspending computer or IT systems. Likewise, articles 635-bis, 635-ter, 635-quarter and 635-quinquies of the Criminal Code shall be taken into consideration for their scope of application concerning the damage of information, data and computer software.

With regard to employee monitoring, the main provision is represented by article 4 of the Statute of Workers. In particular, CCTV systems and the other instruments from which it derives the possibility of remote control of workers' activity can be used exclusively for organisational and production needs, for the safety of the work and for the protection of the company assets and can be installed subject to the collective agreement stipulated by the company trade union representatives. Alternatively, in the case of companies with production units located in different zones of the same region or in more than one region, such agreement may be stipulated by the comparatively more representative trade unions at the national level. In the absence of agreement, the above-mentioned instruments may be installed subject to authorisation from the territorial office of the National Labour Inspectorate or, alternatively, in the case of companies with production units located in the areas of most territorial offices, of the headquarters of the National Labour Inspectorate.

8 PII formats

What forms of PII are covered by the law?

The GDPR ensures the protection of all personal data; namely, any information relating to an identified or identifiable natural person. An identifiable natural person is 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, the GDPR covers all PII irrespective of the format in which it is processed.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

No. The reach of the Code and its application is not limited to data controllers and data processors established within Italian territory. In fact, section 5 of the Code provides for the applicable privacy law principle to be in force in Italy. According to this principle, Italian privacy law will continue to apply in two scenarios:

- data controllers or data processors established either in the Italian state's territory or in a place that is under the Italian state's sovereignty; or
- data controllers or data processors established in a country outside the EU and making use in connection with the processing of equipment, whether electronic or otherwise, situated in the Italian state's territory, unless such equipment is used only for the purposes of transit through the territory of the EU.

10 Covered uses of PII

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

All personal data processing is covered by the GDPR (ie, any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (see article 4(2) of the GDPR)).

The GDPR maintains the fundamental distinction between data controllers and the data processors set by the DPD.

Data controllers are those subjects having fully autonomous decision-making powers – also jointly with another data controller – in respect of the purposes and mechanisms of data processing operations as also related to security matters.

Data processors, where designated, are selected among entities that can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to processing as also related to security matters. Data processors act on behalf of the data controller.

Their duties are different in line with their different roles. In particular, data controllers have to implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR. Although a similar obligation is imposed upon data processors – in fact the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner

that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject – some obligations are imposed only on data controllers (eg, privacy-by-design, data protection impact assessments, different records of processing activities, etc).

Legitimate processing of PII

11 Legitimate processing – grounds

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

Yes. Article 6 of the GDPR provides that processing shall be lawful only where:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

However, article 6(2) of the GDPR leaves the margin of intervention to member states with regard to processing activities deemed lawful because necessary for compliance with a legal obligation and for the performance of a task carried out in the public interest. Finally, article 6(4) sets the parameters to assess the lawfulness of 'data reuse' activities.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Yes. The GDPR sets a higher threshold for lawfully processing special categories of data (ie, sensitive data). In particular, according to article 9 of the GDPR, the processing of personal 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 shall be prohibited, unless:

- the data subject has given explicit consent to the processing of the 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 insofar as it is authorised by EU or 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;
- processing relates to personal data which 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 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; or
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Furthermore, some important guidelines issued by the IDPA expressly provide more stringent rules when the processing refers to sensitive data, biometric data, bank information, employees' personal data processed in the employment context, mobile payments and so on.

Biometric data processing is currently regulated by rules regarding processing operations that involve specific risks. As a consequence, the processing of biometric data shall be allowed only in accordance with such measures and precautions as are laid down to safeguard data subjects, if the processing is likely to present specific risks to data subjects' fundamental rights and freedoms. Having regard to the nature of the data, the arrangements apply to the processing or the effects the latter may produce.

With specific reference to the processing of biometric data, the IDPA issued a general resolution on biometric identification and graphometric signatures. This general resolution introduces important news, general rules and a number of specific cases of deregulation. In the meantime, technological development and a general enlargement of the scope of biometric processing is currently pushing the IDPA to update its general resolution on biometrics, also in line with the new openings provided for by the GDPR on the matter.

Moreover, other specific rules can be found in general resolutions issued by the IDPA with particular regard to the data processing carried out in an employment context, bank and credit information processing and mobile payments.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Pursuant to article 13 of the GDPR, data controllers are required to preliminarily inform data subjects about any useful information regarding the processing of their data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

When the PII is collected from the data subject, the information notice to be provided to the data subjects must contain the following information:

- 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 is intended, as well as the legal basis for the processing;
- where the processing is based on point (f) of article 6(1), the legitimate interests pursued by the controller or by a 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 Commission;
- 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 the IDPA;
- 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.

14 Exemption from notification

When is notice not required?

Under a general point of view, pursuant to article 14(5) of the GDPR, whenever the personal data is not collected from the data subject the information notice to data subjects is not required when:

- the data subject already has the information;
- the provision of such information 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) or insofar as the obligation referred to in paragraph 1 of this article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases, the 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 is expressly laid down by European Union or member state law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by European Union or member state law, including a statutory obligation of secrecy.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Yes. Data subjects may choose to give their consent to the processing as a whole or to one or more of the operations thereof.

Moreover, pursuant to article 15-22 of the GDPR, data subjects, among other things, have the right to control their personal data by asking for and obtaining:

- the updating, rectification or integration of personal data; and
- the erasure, anonymisation or blocking of personal data.

Finally, they have the right to data portability, to restriction of the processing, to object and not to be subject to a decision based solely on automated processing.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Yes. The GDPR expressly establishes that personal data undergoing processing shall be accurate and, when necessary, up to date; relevant; complete; and not excessive in relation to the purposes for which it is collected or subsequently processed (see article 4(1)(d) of the GDPR).

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

As highlighted in question 1, the general principle provided for by the GDPR is that personal data undergoing processing shall be kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data was collected or subsequently processed (article 5 of the GDPR). Therefore, from a general point of view, the GDPR does not provide for a specific period for personal data retention. However, in order to ensure an elevated level of data protection, the data controller is required to put in place proper procedures to delete, destroy or make anonymous any personal data that is no longer useful for the purposes for which it has been collected and processed.

Moreover, in certain cases the Code establishes a specific data retention period, such as traffic data in the telecom sector, data captured by video surveillance systems, biometric data, banking and credit information and so on.

Note that some of the extended retention periods were grounded upon Directive 2006/24/EC (the Data Retention Directive), known for having been declared invalid for violation of fundamental rights by the Court of Justice of the EU.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes. The finality principle or purpose limitation principle is part of the EU legal framework for data protection. Pursuant to article 5(1)(b) of the GDPR, personal data shall becollected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The GDPR provides that 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 (in accordance with article 89 of the GDPR).

Moreover, the GDPR implements a 'data reuse' test whose elements are set by article 6(4) of the GDPR.

Security

20 Security obligations

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

Pursuant to article 32 of the GDPR, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In doing this, they should take into account:

- the state of the art;
- the costs of implementation;
- the nature, scope, context and purposes of processing;
- the risk of varying likelihood; and
- severity for the rights and freedoms of natural persons.

The Regulation itself deems as appropriate the following measures:

- 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 in a timely manner 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.

21 Notification of data breach

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 GDPR, in case of a personal data breach, the controller shall notify without undue delay the personal data breach to the competent DPA, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In addition, 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 data subject without undue delay.

With regard to sector-specific obligations, pursuant to section 32-bis of the Code, data breach notification is deemed as a mandatory obligation for providers of publicly available electronic communications services, who shall notify security breaches to the IDPA without undue delay. Moreover, when the personal data breach is likely to be detrimental to the personal data or privacy of the contracting party or another individual, the provider shall also notify the contracting party or the individual of the said breach without delay. The notification above shall not be required if the provider has demonstrated to the

IDPA that he or she implemented technological protection measures that render the data unintelligible to any entity that is not authorised to access it, and that said measures were applied to the data affected by the breach.

Moreover, pursuant to sector-specific general resolutions issued by the IDPA, data breach notification is also a mandatory requirement for:

- banks and other companies belonging to a bank group – including third companies operating in outsourcing – that process bank information; and
- data controllers that process biometric data.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

According to article 37 of the GDPR, the controller and the processor shall designate a data protection officer (DPO) in any case 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 which, 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 and personal data relating to criminal convictions and offences.

The appointed DPO shall, at least:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations arising from the GDPR and from other EU or member state data protection provisions;
- 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;
- provide advice where requested as regards the data protection impact assessment and monitor its performance;
- cooperate with the DPAs; and
- 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.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Yes. Under article 30 of the GDPR, data controllers and processors are required to maintain a record of processing activities under their responsibility. These records are slightly different, in line with their roles. Controllers' records are consequently more detailed, having to specify, inter alia, the purpose of the processing, the description of the categories of data subjects and data processed, the categories of recipients, the security measures envisaged and so on.

Furthermore, a specific exemption is set by article 30 where the enterprise is employing fewer than 250 persons unless the processing carried 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 personal data relating to criminal convictions and offences.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Yes. In particular, article 25 of the GDPR provides that data controllers shall implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards within processing operations in order to protect the rights of data subjects. Moreover, pursuant to the same article, data controllers shall implement appropriate technical and organisational measures for ensuring that, by default and from the outset, only personal data which is necessary for each specific purpose of the processing is processed.

With regard to data protection impact assessments (DPIAs), article 35 of the GDPR provides that where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. In this case, the EU legislator has demanded controllers to self-assess the degree of risk for data subjects, in line with the principle of accountability.

Where a DPIA reveals that the processing would result in a high risk in the absence of mitigation measures, the controller shall consult the competent DPA.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

No. Under the GDPR it is no longer necessary for controllers or processors to register with the DPA.

26 Formalities

What are the formalities for registration?

Not applicable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

According to the GDPR, data controllers and processors shall notify to the DPA (and to data subjects) data breaches that have occurred (see question 21). Moreover, according to article 37, controllers and processors shall publish and notify to the DPA the contact details of the DPO.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Where processing activities have to be carried out by an outsourcer on behalf of the controller, the former shall be chosen only among those providing sufficient guarantees. Moreover, processing by a processor shall be governed by a contract or other legal act as provided by article 28 of the GDPR.

Where the purposes and means of the processing are determined by the outsourcer, it may be considered an autonomous data controller,

triggering the application of all the provisions of the GDPR applicable to data controllers.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

The GDPR provides a specific 'right to restriction of processing' that may involve restrictions on the disclosure of personal data. However, the right to restriction of processing shall be defined by member states (see question 1).

As a general rule under the Code regime, communication and dissemination shall be prohibited if an order to this effect has been issued by either the IDPA or judicial authorities, as well as with regard to personal data that must be erased by order, or else upon expiry of the term of its retention (no longer than is necessary for the purposes for which the data is collected or subsequently processed); and for purposes other than those specified in the notification, whenever the latter is to be submitted. This shall be without prejudice to communication and dissemination of the data as requested, pursuant to law, by police, judicial authorities, intelligence and security agencies and other public bodies, for the purposes of defence or relating to state security, or for the prevention, detection or suppression of offences.

Nevertheless, apart from the above, PII may be communicated to third-party data controllers only where the data subjects have given their express consent to the communication, after being properly informed in this regard.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

As a general principle, according to both the DP Directive and the GDPR, data transfer inside the EU and EEA is permitted and not restricted. The legal framework becomes quite different with specific reference to data transfer abroad, outside the EU.

According to the GDPR, data transfer to third countries located outside the EU and EEA is not always allowed. In fact, the main tools allowing international data transfers are:

- standard contractual clauses (SCCs);
- binding corporate rules (BCRs);
- an approved code of conduct;
- an approved certification mechanism; and
- privacy shield and further adequate protection decisions.

Moreover, the GPDR provides for further specific derogations that may legitimate the data transfer abroad, also in the absence of the tools highlighted above. For instance, PII may be transferred from the Italian state's territory to countries outside the EU – temporarily or not and in any form and by any means whatsoever – when the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject. Additionally, a cross-border data transfer can be carried out when it is necessary to safeguard a substantial public interest that is referred to by laws or regulations or when the transfer is necessary to safeguard a third party's life or bodily integrity.

Other cases are represented by the necessity of establishing or defending a legal claim, provided that the data is transferred exclusively for said purposes and for no longer than is necessary in compliance with the legislation in force applying to business and industrial secrecy.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

In certain cases, cross-border data transfer requires notification to or authorisation from the IDPA.

With specific reference to BCRs, it is necessary to obtain authorisation or approval from the IDPA, while with regard to SCCs, it is necessary to notify their use to the IDPA only where modifications to the format issued by the European Commission are made.

36 Further transfer

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

Yes.

Rights of individuals

37 Access

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

According to the GDPR's provisions, data subjects have the right to obtain from the controller confirmation as to whether or not PII concerning him or her is being processed, and access to their PII.

38 Other rights

Do individuals have other substantive rights?

Yes. Pursuant to the GDPR, data subjects have the right to:

- access their PII, obtaining evidence of the purposes pursued by the controller, the categories of data involved, the recipients to whom they may be disclosed, the applicable storage period and the existence of automated decision-making processes;
- have incorrect PII referred to them rectified without delay;
- have their PII erased in the cases provided for by the law;
- obtain restrictions to processing, where possible;
- request portability of the data provided, ie, receiving it in a structured, commonly used and machine-readable format, also for transmitting such data to another controller, without any hindrance, in all situations where it is required by the law in force; and
- lodge a complaint to the IDPA.

39 Compensation

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 GPDR provides that any person who has suffered material or non-material damage as a result of data protection provisions shall have the right to receive compensation from the controller or processor for the damage suffered.

Under the Code regime, section 15 of the Code – entitled Damage Caused on Account of the Processing – provided that: 'Whoever causes damage to another as a consequence of the processing of personal data shall be liable to pay damages pursuant to section 2050 of the Civil Code.' In turn, section 2050 of the Civil Code – entitled Liability for Dangerous Activities' Practices – establishes that whoever causes damage to another during the carrying out of any activity that is considered dangerous owing to its nature or the means used, shall indemnify the injured party, in case he or she does not prove to have taken all the necessary measures in order to avoid the damage. In this respect, according to section 2050 of the Civil Code, the Italian legislator would provide a specific civil liability in case of data breach, where a reversal of the burden of proof occurs. In other words, whoever processes the data and causes its breach has the burden to prove that he or she has done everything possible in order to avoid the breach.

40 Enforcement

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

The rights referred to in question 38 may be enforced either by filing a lawsuit or by lodging a complaint with the IDPA. The right to receive a payment for the damage suffered as a consequence of data processing may be enforced only by filing a lawsuit.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Generally speaking, no.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, PII owners can appeal against orders of the supervisory authority to the courts.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Note that the Italian Privacy Code is also the means of implementation of the Directive 2002/58/EU (the ePrivacy Directive).

Cookies

With specific reference to the use of cookies, the Privacy Code establishes that it shall be prohibited to use an electronic communications network in order to access information stored in the terminal equipment of a contracting party or user, store information or monitor the operations performed by the user. In other words, a provider may only use cookies that are strictly necessary to operate the service as per users' requests. In all other cases and for each additional purpose, the service provider shall inform the users and obtain their previous consent in order to lawfully use cookies differing from those strictly necessary for the service requested (see section 122(1) of the Privacy Code).

Moreover, it is also established that in order to determine the simplified arrangements, the IDPA shall also take account of the proposals put forward by the consumer and industry associations involved with the largest representation at national level in order to ensure that the mechanisms implemented make the contracting party or user actually aware.

In this regard, the IDPA has issued general resolution No. 229 of 8 May 2014, by means of which the Authority wanted to stop the installation of cookies for both profiling and marketing purposes in the absence of a previous information notice to users or the acquisition of their consent. Consequently, whoever browses online has to freely and consciously decide to prevent or to allow the use of their own information, gathered during browsing a website, in order to receive profiled advertising.

With reference to the obligation of keeping track of users' consent, the website administrator can use a technical cookie, avoiding having to provide twice the simplified information to those users who have already visited the website.

Online profiling by technical means different from cookies

By means of general resolution No. 161 of 19 March 2015 – the Guidelines on personal data processing for profiling purposes (the Guidelines) – the IDPA issued a set of rules that data controllers must follow when processing online users' PII for profiling purposes. In more detail, the IDPA has established that whoever works on the internet shall provide users with clear and complete information, require and obtain the data subjects' consent, which may be withdrawn at any time, and also offer concrete protections to those who do not have a specific account to access the services provided.

The rules provided for by the Guidelines shall apply to all subjects providing online services (such as a search engine, email, online maps, social networks, e-payment and cloud computing) and that are established on the Italian state's territory:

- Protection for each user: companies shall protect the privacy of both registered users and users who do not have a specific account to access the services provided.
- Information notice: the information notice on the data processing shall be clear, complete, exhaustive and visible, starting from the first web page.
- Consent: the processing of users' personal data must be carried out only in the presence of the users' informed consent. Such consent may be given through the modalities and criteria provided for by the Guidelines.
- Data retention: it is necessary to establish an ad hoc period of data retention proportioned to the specific purposes of the processing.

Update and trends

The emerging trends of data protection in Italy can be divided into two categories: the ones arising from the coming into force of the GDPR and the ones following the latest technological innovations.

Among the GDPR-related trends, we may identify an increasing use of the data comptroller's legitimate interest as legal grounds for the processing; in this sense, the GDPR is changing the perspective, as a prior approval with a 'balancing of interest' decision by the Italian Supervisory Authority was required under the Privacy Code. Furthermore, the introduction of a general right to portability of personal data is compelling many players to set up technological systems and procedures to deal with it; the consequence is an increasing attempt to identify some interoperable formats that may allow a fast and safe portability of data.

The second category is directly linked with the proliferation of studies and practical implementations of blockchain technology. Blockchain's revolutionary approach is already changing our everyday life, and the implications are becoming more and more relevant. However, data protection's approach and principles envisaged by the GDPR are simply clashing with the inherent nature of blockchain and distributed ledger technologies, creating serious risks for companies deciding to make use of it, and eventually discouraging investments.

Finally, the IDPA is reorganising in order to face the challenges brought by the GDPR in terms of renovated efforts required to the authorities to effectively enforce the Regulation.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

With specific reference to marketing matter, different regimes apply depending on the case.

Opt-in regime

The use of automated calling or communications systems without human intervention for the purposes of direct marketing or sending advertising materials, or for carrying out market surveys or interactive business communication, shall only be allowed with the contracting party's or user's consent (this shall apply also to electronic communications performed by email, facsimile or MMS or SMS-type messages or other means for the same purposes).

Opt-out regime

With reference to the mail and phone numbers taken from public registers, lists, records and publicly available documents, the related processing in question could be performed without the data subject's consent, provided that the latter has not objected or does not object to the processing by means of his or her registration within the Opposition Register, which is similar to a Robinson list. A similar register has not yet been implemented for mailing services.

Note that section 130(4) of the Privacy Code introduces a 'soft spam' hypothesis. In this case, where a data owner uses electronic mail contacts for direct marketing and contact details have been supplied by a data subject in the context of the sale of a product or service, said data controller may fail to request the data subject's consent, on condition that the services are similar to those that have been the subject of the sale, and the data subject, after being adequately informed, does not object to said use.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

With regard to cloud computing, the lack of specific provisions is balanced against the guidance provided for by the Working Party 29 and the IDPA.

In particular, the IDPA issued specific guidelines dealing with cloud computing in May 2012, establishing that where a company, acting as the data controller, moves part or the whole of its processing operations concerning personal data to the cloud, it should appoint the cloud service provider as the data processor. This provision is clearly aimed at extending both Italian jurisdiction and the IDPA's control to those hypotheses in which even personal data transferred abroad is processed by third subjects outside Italian state territory.

With regard to data security, the IDPA recommends to clients (data controllers) of a cloud service to make sure that data is accessible at any time and only by those authorised to do so. Moreover, the technology and level of encryption used during data flows and transmissions should also be taken into account when assessing the overall level of security.

Finally, the IDPA focused its attention upon data subjects' rights and their exercise in cloud architectures. To fulfil its legal obligations toward data subjects, the client of a cloud-based service will have to adequately supervise the provider and possible sub-processor of the provider.

PANETTA & ASSOCIATI
STUDIO LEGALE

Rocco Panetta **r.panetta@panetta.net**
Federico Sartore **f.sartore@panetta.net**

Via Arenula 83,
Rome 00186
Italy

Tel: +39 06 68210129
www.panetta.net

Japan

Akemi Suzuki and Tomohiro Sekiguchi
Nagashima Ohno & Tsunematsu

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The Act on the Protection of Personal Information of 2003, as amended (the APPI), sits at the centre of Japan's regime for the protection of PII. Serving as a comprehensive, cross-sectoral framework, the APPI regulates private businesses using databases of PII and is generally considered to embody the eight basic principles under the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Use of PII by the public sector is regulated by separate statutes or local ordinances providing for rules for protection of PII held by governmental authorities.

In September 2015, the first-ever significant amendment to the APPI (the Amendment) since its introduction was promulgated. The Amendment aims to eliminate the ambiguity of the current regulatory framework and facilitate the proper use of personal data by businesses while strengthening the protection of privacy. It also aims to address global data transfers and harmonise Japan's data protection regime with that of other major jurisdictions. The Amendment was fully implemented on 30 May 2017.

The APPI, as amended by the Amendment, is implemented by cross-sectoral administrative guidelines prepared by the Personal Information Protection Commission (the Commission). With respect to certain sectors, such as medical, financial and telecommunications, the Commission and the relevant governmental 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 PII.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Commission was established on 1 January 2016 as a cross-sectoral, independent governmental body to oversee the APPI. The Commission has the following powers under the APPI:

- to require reports concerning the handling of PII or anonymised information from PII data users (as defined in question 10) or private business operators using database, etc, of anonymised information (for the purposes of this chapter, anonymised information users);
- to conduct an on-site inspection of offices or other premises of PII data users and anonymised information users in order to raise questions and inspect records with respect to their handling of PII or anonymised information;
- to give 'guidance' or 'advice' necessary for the handling of PII or anonymised information to PII data users and anonymised information users;
- upon violation of certain obligations of any PII data users or anonymised information users 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 governmental ministry deems 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 as mentioned above to certain governmental ministries in cases where the Commission deems it necessary to be able to give 'guidance' or 'advice' to PII data users or anonymised information users effectively.

3 Legal obligations of data protection authority

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

Under the APPI, in cases where governmental ministries deem necessary to ensure the proper handling of personal information, such governmental ministries may request the Commission to take appropriate measures in accordance with the provisions of the APPI.

In addition, 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 set forth in the APPI. Upon request from the foreign authorities, the Commission may consent that the information provided by the Commission be used for an investigation of a foreign criminal case, subject to certain exceptions.

4 Breaches of data protection

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:

- a PII data user or an anonymised information user fails to comply with any order issued by the Commission (subject to penal servitude of up to six months or a criminal fine of up to ¥300,000);
- a PII data user or an anonymised information user fails to submit reports, or submits untrue reports, as required by the Commission (subject to a criminal fine of up to ¥300,000);
- a PII data user or an anonymised information user refuses or interrupts an on-site inspection of the offices or other premises by the Commission (subject to a criminal fine of up to ¥300,000); or
- any current or former officer, employee or representative of a PII data user provides to a third party or steals information from a PII database he or she handled in connection with the business of the PII data user with a view to providing 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 PII data user or an anonymised information user that is a judicial entity, then the entity itself may also be held liable for a criminal fine.

Scope

5 Exempt sectors and institutions

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

The APPI contains notable exemptions as follows:

- In respect of fundamental constitutional rights, media outlets and journalists, universities and other academic institutions, religious groups and political parties are exempt from the APPI to the extent of the processing of personal data for purposes of journalism, academic research and religious and political activities, respectively.
- Use of PII for personal purposes is outside the scope of the APPI. Use of PII by not-for-profit organisations or sole proprietorships is within the scope of the APPI.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

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.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Use of personal information by governmental sectors is regulated by the Act on the Protection of Personal Information Held by Administrative Organs of 2003, the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies of 2003 and various local ordinances providing rules for the protection of PII held by local governments. In addition, the Act on Utilisation of Numbers to Identify Specific Individuals in Administrative Process provides rules concerning the use of personal information acquired through the use of the individual social security and tax numbering system called My Number. With respect to employee monitoring, while there is no statute regulating employee monitoring in Japan, the Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines) provide for the best practice in cases of carrying out employee monitoring.

8 PII formats

What forms of PII are covered by the law?

In terms of forms of PII, the use of 'database, etc' of PII (PII database) is covered by the APPI. PII database includes not only electronic databases but also 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, PII 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 PII. PII 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. PII comprising a PII database is called PII data.

In addition, the Amendment has introduced the concept of 'anonymised information'; that is, personal information of a particular individual that has been irreversibly processed in such a manner that the individual is no longer identifiable. Anonymised information that complies with the requirements of the techniques and processes for anonymisation under the Amendment is not considered PII. Anonymised information 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.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The APPI has limited extraterritorial application. Specifically, the APPI is applicable to foreign PII data users or anonymised information users when they use or process, outside of Japan:

- PII of individuals residing in Japan as was obtained in connection with the provision of goods or services by the PII data users to Japanese resident individuals; or
- anonymised information produced by the PII data users based on such PII.

Separately, PII of individuals residing outside of Japan is considered to be protected under the APPI as long as such PII is held by private business operators established or operating in Japan.

10 Covered uses of PII

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

The APPI distinguishes between (i) obligations imposed on all private business operators using PII database (for the purposes of this chapter, called PII data users); and (ii) obligations imposed only on those PII data users who control the relevant PII data (for the purposes of this chapter, called PII data owners). Generally, service providers are subject to the obligations of PII data users but not subject to the obligations of PII data owners.

The obligations of all PII data users mentioned in (i) include:

- to specify the purposes for which the PII is used and to process the PII only to the extent necessary for achieving such specified purposes (see question 11);
- to notify the relevant individual of, or publicise, the purposes of use prior to or at the time of collecting PII (see question 13);
- not to use deceptive or wrongful means in collecting PII (see question 11);
- to obtain the consent of the individual prior to collecting sensitive personal information (subject to certain exceptions) (see question 12);
- to endeavour to keep its PII data accurate and up to date to the extent necessary for the purposes of use, and erase, without delay, its PII data that is no longer needed to be used (see question 16);
- to undertake necessary and appropriate measures to safeguard the PII data it holds (see question 20);
- to conduct necessary and appropriate supervision over its employees and its service providers who process its PII data (see question 20);
- not to disclose the PII data to any third party without the consent of the individual (subject to certain exemptions) (see question 32);
- to prepare and keep records of third-party transfers of personal data (subject to certain exceptions) (see question 23);
- 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 (see question 23); and
- not to conduct cross-border transfers of personal data without the consent of the individual (subject to certain exceptions) (see question 34).

The PII data owners mentioned in (ii) have additional and more stringent obligations, which are imposed only with respect to such PII data for which a PII data owner has the right to provide a copy of, modify (correct, add or delete), discontinue using, erase or discontinue disclosure to third parties (retained PII data):

- to make accessible to the relevant individual certain information regarding the retained PII data (see question 13);
- to provide, without delay, a copy of retained PII data to the relevant individual upon his or her request (see question 37);
- to correct, add or delete the retained PII data to the extent necessary for achieving the purposes of use upon the request of the relevant individual (see question 15);
- to discontinue the use of or erase such retained PII data upon the request of the relevant individual if such use is or was made, or the retained PII data in question was obtained, in violation of the APPI (see question 15); and
- to discontinue disclosure of retained PII data to third parties upon the request of the relevant individual if such disclosure is or was made in violation of the APPI (see question 15).

The following are excluded from the retained PII data and therefore do not trigger the above-mentioned obligations of PII data owners:

- any PII data where the existence or absence of such PII 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 would impede criminal investigations or public safety; and
- any PII data that is to be erased from the PII database within six months after it became part of the PII database.

Legitimate processing of PII

11 Legitimate processing – grounds

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

The APPI does not contain specific criteria for legitimate data collection or processing. The APPI does, however, prohibit the collection of PII 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. Processing of PII beyond the extent necessary for such purposes of use without the relevant individual's prior consent is also prohibited, subject to limited exceptions.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The APPI imposes stringent rules for 'sensitive personal information' (*you hairyo kojin jouhou*), which includes race, beliefs, social status, medical history, criminal records and the fact of having been a victim of a crime and disabilities. Collection or disclosure under the 'opt-out' mechanism of sensitive personal information without the consent of the relevant individual will be generally prohibited.

In addition, the administrative guidelines for the financial sector provide for a similar category of 'sensitive information' (*kibi jouhou*). 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.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

There are several notification requirements under the APPI.

First, the APPI requires all PII data users to notify individuals of, or make available to individuals, the purpose for which their PII data is used, promptly after the collection of the PII, unless such purpose was publicised prior to the collection of the PII. Alternatively, such purpose must be expressly stated in writing if collecting PII provided in writing by the individual directly.

Second, when a PII data user is to disclose PII data to third parties without the individual's consent under the 'opt-out' mechanism, one of the requirements that the PII data user must satisfy is that certain information regarding the third-party disclosure is notified, or made easily accessible, to the individual prior to such disclosure (see question 33). Such information includes types of information being disclosed and the manner of disclosure.

Third, the APPI requires each PII data owner to keep certain information accessible to those individuals whose retained PII data is held. Such information includes: the name of the PII data owner; all purposes for which retained PII data held by the PII data owner is generally used; and procedures for submitting a request or filing complaints to the PII data owner. If, based on such information, an individual requests the specific purposes of use of his or her retained PII data, the PII data owner is required to notify, without delay, the individual of such purposes.

14 Exemption from notification

When is notice not required?

There is an exception to the first notice requirement mentioned in question 13 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 PII data user; and the purposes of use are evident from the context of the collection of the relevant PII data.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Upon request from an individual, a PII data owner must:

- disclose, without delay, retained PII data in written form to the relevant individual upon his or her request (see question 37);
- correct, add or delete the retained PII data to the extent necessary for achieving the purposes of use upon request from the relevant individual;
- discontinue the use of or erase the retained PII data upon the request of the relevant individual if such use is or was made, or the retained PII data in question was obtained, in violation of the APPI; and
- discontinue disclosure to third parties of retained PII data upon the request of the relevant individual if such disclosure is or was made in violation of the APPI.

An exemption from the third and fourth obligations mentioned above is available where the discontinuance or erasure costs significantly or otherwise impose hardships on the PII data owner and one or more alternative measures to protect the individual's interests are taken.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The APPI requires all PII data users to endeavour to:

- keep the PII data they hold accurate and up to date to the extent necessary for the purposes for which the PII data is to be used; and
- erase, without delay, such PII data that is no longer needed.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

No. PII data may be held as long as is necessary for the purposes for which it is used. Under the APPI, PII data users must endeavour to erase, without delay, such PII data that is no longer needed to be used.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

PII can generally be used only to the extent necessary to achieve such specified purposes as notified or made available to the relevant individual in a manner mentioned in question 13. 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 are applicable to, for instance, the use of PII 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 consent of the affected individual.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

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.

PII may be used for such amended purposes, provided that the amended purposes be notified or made available to the affected individuals.

Security

20 Security obligations

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

The APPI provides that all PII 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 PII data they hold or process; and conduct necessary and appropriate supervision over their employees and service providers who process such PII data. What constitutes 'necessary and appropriate' security measures is elaborated on in 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.

Some of the sector-specific guidelines, such as the administrative guidelines for the financial sector, provide for more stringent requirements on security measures.

21 Notification of data breach

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 APPI does not include obligations to notify the regulators or affected individuals of any breaches of security. However, upon the occurrence of any such breach, notification to the Commission, governmental ministries delegated by the Commission or an accredited personal information protection organisation, if applicable, is generally required or recommended under the Commission Guidelines. Such reporting is not required if the compromised personal data is considered not to have leaked; for instance, if the relevant personal data is securely encrypted, was recovered before a third party had access to it or was destroyed and no third party is reasonably expected to view the relevant personal data. Regulatory reporting is also not required if the relevant data breach is minor; for instance, erroneous transmission of emails or facsimiles or wrong delivery of packages where the compromised personal data is limited to the names of the sender and recipient.

In addition, under the Commission Guidelines, notification of data breaches to data subjects may be necessary depending on the subject and manner of such breaches. If a particular data breach is not expected to result in damage to the relevant data subjects, such as where the breached personal data was securely encrypted, notification to data subjects will not be necessary.

Some of the sector-specific administrative guidelines provide for more stringent requirements on notification of data breaches. For instance, under the administrative guidelines for the financial sector, upon the occurrence of any data breach, notifications to both the relevant government ministries and the data subject are required for PII data users in the financial sector without any exceptions.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

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.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

PII data users are generally required under the Commission Guidelines to establish internal processes to safeguard PII data.

Under the APPI, PII data users that have disclosed PII data to third parties must generally keep records of such disclosure. In addition, PII data users receiving PII data from third parties rather than the relevant individuals must generally verify how the PII data was acquired by such third parties and keep records of such verification.

The foregoing obligation is not applicable to disclosure of PII data to outsourced processing service providers (see question 32), as part of mergers and acquisitions (M&A) transactions (see question 33) or for joint use (see question 33), as long as the disclosure is not subject to the cross-border transfer restrictions.

24 New processing regulations

Are there any obligations in relation to new processing operations?

No. However, the Commission Guidelines generally require that, when implementing security measures to safeguard the PII data it holds or processes, each PII data user should consider the degree of the impact of any unauthorised disclosure or other incident on the right or interest of one or more data subjects affected by such an incident.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

Under the APPI, PII data users who disclose PII data (other than sensitive personal information) under the 'opt-out' mechanism are required to submit a notification to the Commission prior to such disclosure. According to the Commission, the primary target of this requirement is mailing list brokers.

26 Formalities

What are the formalities for registration?

PII data users who disclose PII data under the 'opt-out' mechanism mentioned in question 25 are required to notify the Commission, in a prescribed format, of the categories of personal data to be disclosed, the method of disclosure, the manner in which the relevant individual may request to cancel such 'opt-out' disclosure to the PII data users and other designated matters. Upon receipt of such notification, the Commission will publicise certain information included in the notification.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

No penalties are statutorily provided for the failure to submit a notification of the 'opt-out' disclosure mentioned in questions 25 and 26.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

Notifications of the 'opt-out' disclosure mentioned in questions 25 and 26 are partially made public on the Commission's website.

30 Effect of registration

Does an entry on the register have any specific legal effect?

A notification of the 'opt-out' disclosure mentioned in questions 25 and 26 is a requirement to lawfully disclose PII data (other than sensitive personal information) to third parties without the relevant individual's consent under the 'opt-out' mechanism.

31 Other transparency duties

Are there any other public transparency duties?

Apart from the matters required to notify individuals as mentioned in question 13, the Commission Guidelines recommend that PII data users make public an outline of the processing of PII data such as whether PII data users outsource the processing of PII data and the contents of the processing to be outsourced.

In addition, the administrative guidelines for the financial sector recommend that PII data users make public:

- the purpose of use of personal information specified in accordance with types of customers;
- whether PII data users outsource the processing of PII data;
- the contents of the processing to be outsourced;
- the types of personal information;
- the methods of obtaining personal information; and
- a statement to the effect that upon request from individuals, the use of retained PII data will be discontinued.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The APPI generally prohibits disclosure of PII data to third parties without the relevant individual's consent. As an exception to such prohibition, the transfer of all or part of PII data to persons that provide outsourced processing services is permitted to the extent such services are necessary for achieving the permitted purposes of use. PII data users are required to engage in 'necessary and appropriate' supervision over such service providers in order to safeguard the transferred PII data. Necessary and appropriate supervision by PII data users 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.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

In principle, the APPI prohibits disclosure of PII to a third party without the individual's consent. Important exceptions to the general prohibition include the following, in addition to disclosure for outsourced processing services mentioned in question 32 above:

- disclosure under the 'opt-out' mechanism: a PII data user may disclose PII data to third parties without the individual's consent, provided that it is prepared to cease such disclosure upon request from the individual; certain information regarding such disclosure is notified, or made easily accessible, to the individual prior to such disclosure; and such information is notified to the Commission in advance;
- transfer in M&A transactions: PII data may be transferred without the consent of the individual in connection with the transfer of business as a result of a merger or other transactions; and
- disclosure for joint use: a PII data user may disclose PII 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 prior to such disclosure. Such disclosure is most typically made when sharing customer information among group companies in order to provide seamless services within the permitted purposes of use. Information required to be notified or made available includes items of PII data to be jointly used, the scope of third parties who would jointly use the PII data, the purpose of use by such third parties, and the name of a party responsible for the control of the PII data in question.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Under the APPI, the transfer of PII data to a third party located outside of Japan is generally subject to 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. At the time of writing, no country is designated as such by the Commission. However, according to the joint statement of the Commission and the European Commission published on 31 May 2018, they agreed to intensify their work to complete as soon as possible:

- the designation of the European Economic Area (EEA) by the Commission as a foreign country that has the same level of protection of personal information as Japan; and
- the parallel decision by the European Commission that Japan ensures an adequate level of protection of personal data under article 45 of the EU General Data Protection Regulation (GDPR).

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 PII data users would be required under the APPI. According to the Commission Guidelines, in order for this exception to apply, the PII data user 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. In addition, 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 APEC's Cross Border Privacy Rules (CBPR) system.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, cross-border transfer of PII does not trigger a requirement to notify or obtain authorisation from a supervisory authority.

36 Further transfer

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 PII mentioned in question 34 are applicable to transfers to service providers. They may also be applicable to onward transfers in the sense that the initial PII data users must ensure that not only the transferors of such onward transfers but also their transferees adhere to the cross-border restrictions of the APPI.

Update and trends

The Personal Information Protection Commission and the European Commission are working to finalise the designation of the European Economic Area (EEA) by the Commission as a foreign country that has the same level of protection of personal information as Japan, and the parallel decision by the European Commission that Japan ensures an adequate level of protection of personal data under article 45 of the EU GDPR.

In order to address certain discrepancies between the requirements of the APPI and the GDPR, the Commission has proposed a draft of the administrative guidelines regarding the handling of PII data to be transferred from the EEA should the European Commission decide that Japan ensures an adequate level of protection of PII data (Proposed Guidelines). The outline of the Proposed Guidelines is as follows:

- in cases where PII data transferred from the EEA based on the adequacy decision by the European Commission (EEA data) includes data concerning sex life, sexual orientation or trade union membership, which are categorised as special categories of PII data under the GDPR, such EEA data is treated as 'sensitive personal information' (*you hairyo kojin jouhou*) under the APPI (see question 12);
- EEA data is treated as retained PII data under the APPI, regardless of whether or not such EEA data is erased within six months (see question 10);
- (i) when a PII data user receives EEA data from EEA, the PII data user 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); (ii) when a PII data user receives EEA data from another PII data user that received such EEA data from the EEA, the PII data user is also required to confirm and record the original purposes of use of such EEA data; and (iii) in each case of (i) and (ii), the PII data user 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 in accordance with such specified purposes of use;
- in cases where a PII data user proposes to transfer EEA data it received from the EEA to a third party transferee located outside of Japan (ie, onward transfer), the PII data user 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 (see question 34); and
- when a PII data user processes EEA data to create anonymised information under the APPI, the PII data user is required to delete any information that could be used to re-identify the relevant individuals, including any information concerning the method of process for anonymisation.

Rights of individuals

37 Access

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

The APPI imposes on PII data owners obligations to respond to individuals' requests for access to their PII data. Specifically, upon request from individuals, PII data owners are obligated to disclose, without delay, retained PII data of the requesting individuals. 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 proper conduct of the business of the PII owners; or
- result in a violation of other laws.

The Amendment clarifies that individuals have the right to require disclosure of their PII held by PII data owners.

38 Other rights

Do individuals have other substantive rights?

In addition to the obligations set forth in question 15, PII data owners are subject to an obligation to cease disclosure of PII data to third parties if the relevant individual 'opts out' of the third-party disclosure.

Under the Amendment, individuals have the right to require PII data owners to correct, add or delete inaccurate retained PII regarding the individuals, to discontinue the use of or erasure of the retained PII data that is used or was collected in violation of the APPI, or discontinue unlawful disclosure to third parties of retained PII data.

39 Compensation

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 PII data users' obligation to compensate individuals upon a breach of the APPI. However, pursuant to 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 PII 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.

40 Enforcement

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

Individuals' right to monetary compensation (mentioned in question 39) is enforced through the judicial system. With regard to violations by PII data owners of the obligations described in questions 37 and 38, individuals may exercise their rights described in questions 37 and 38 through the judicial system, provided that they first request the relevant PII data users to comply with such obligations and two weeks have passed after such request was made. Separately, the Commission may recommend PII 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

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Not applicable.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Administrative law in Japan usually provides for an appeal of a governmental ministry's decision to a court with proper jurisdiction. Therefore, if the Commission or the relevant governmental ministry to which powers of the Commission are duly delegated by the Commission takes administrative actions against a PII data user, the PII data user will generally be able to challenge the actions judicially.

Specific data processing

43 Internet use

Describe 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 APPI.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Unsolicited marketing by email is regulated principally by the Act on Regulation of Transmission of Specified Electronic Mail. Pursuant to the Act, marketing emails can be sent only to a recipient who has 'opted in' to receive them; who has provided the sender with his or her email address in writing (for instance, by providing a business card); who has a business relationship with the sender; or who makes his or her email address available on the internet for business purposes. In addition, 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.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

The Commission has published its stance that the use of cloud server services to store PII data does not constitute disclosure to outsourced processing service providers as long as it is ensured by contract or other-wise that the service providers are properly restricted from accessing PII data stored on their servers. If the use of a particular cloud computing service is considered to constitute disclosure to outsourced processing service providers, PII data users are required to engage in 'necessary and appropriate' supervision over the cloud service providers in order to safeguard the transferred PII data (see question 32). Additionally, PII data users 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 (see question 34).

NAGASHIMA OHNO & TSUNEMATSU

Akemi Suzuki **akemi_suzuki@noandt.com**
Tomohiro Sekiguchi **tomohiro_sekiguchi@noandt.com**

JP Tower
2-7-2 Marunouchi, Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 3 6889 7000
Fax: +81 3 6889 8000
www.noandt.com

Korea

Seung Soo Choi and Seungmin Jasmine Jung
Jipyong LLC

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Korea has a comprehensive set of laws for the protection of PII. The generally applicable law is the Personal Information Protection Act (the PIPA), which provides for the overall protection of PII. The PIPA was enacted with reference to the OECD guidelines and similar foreign precedents. Other than the PIPA, Korea has sector-specific laws as follows:

- the Credit Information Use and Protection Act (the Credit Information Act) protects credit information used in the finance sector;
- the Act on Promotion of Information and Communications Network Utilisation and Information Protection, etc (the Network Act) governs the information communication technology sector; and
- the Medical Service Act applies to the healthcare sector.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Ministry of the Interior and Safety has the authority to oversee compliance with the PIPA and has the powers to investigate any violation of the PIPA. The Financial Services Commission has the authority to oversee the Credit Information Act and has the powers to investigate any violation of the Credit Information Act and impose monetary fines. The Korea Communications Commission has the authority to oversee compliance with the Network Act and has the powers to investigate, regulate and impose monetary fines. The Personal Information Protection Commission is a governmental commission that has the authority to review and determine PII protection policies, to enhance systems and laws and to interpret and implement laws related to PII. The Korea Internet and Security Agency has been delegated authority from the Ministry of the Interior and Safety and the Korea Communications Commission and functions as the governmental agency for the purposes of the PIPA and the Network Act.

3 Legal obligations of data protection authority

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

The PIPA explicitly states that 'unless specifically provided in other laws, the regulation of PII protection shall comply with the PIPA'. This means that it is inevitable for sector-specific authorities such as the Financial Services Commission or the Korea Communications Commission to cooperate with the Ministry of the Interior and Safety, which oversees the PIPA. Although there are no statutory legal obligations, the relevant authorities all cooperate with each other in practice.

4 Breaches of data protection

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

A company that violates the PIPA can be subject to both administrative sanctions and criminal penalties. The Ministry of the Interior and Safety can issue corrective orders such as the termination of any activities that infringe on PII, the temporary suspension of PII processing and the implementation of necessary measures to protect, and prevent any infringement of, PII. Additionally, if the company is determined to have violated any laws related to PII protection, a recommendation for disciplinary measures against the responsible individual (including the representative director and the officer in charge) may be issued. Further, a monetary fine up to 500 million won can be imposed for the loss, theft, leakage, alteration and impairment of a resident registration number.

An individual who discloses or provides unauthorised access to PII acquired in the course of business or impairs, destroys, modifies, falsifies or impairs another person's PII without proper authorisation or beyond the scope of his or her authorisation can be subject to imprisonment for up to five years or a monetary penalty up to 50 million won.

Further, a party that fails to adopt necessary measures to procure security pursuant to the PIPA and, as a result, incurs loss, theft, leakage, alteration or impairment of PII can be subject to imprisonment for up to two years or a monetary penalty up to 10 million won.

Scope

5 Exempt sectors and institutions

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

The PIPA is a general law and applies to all private sectors and government sectors, individuals and companies.

In contrast, the Credit Information Act has limited applicability to financial institutions. The Network Act applies only to information communication service providers.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The PIPA and the Network Act both restrict the unauthorised interception of communications or electronic commerce. Such activities could also be subject to the Protection of Communications Secrets Act or the Criminal Act.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

There are several laws that provide for specific data protection rules by sector. Employee monitoring is governed by the Act on the Promotion

of Workers' Participation and Cooperation. Information in the healthcare sector is subject to the Medical Service Act, National Health Insurance Act, Emergency Medical Service Act and Public Health and Medical Services Act. Information in the finance sector is governed by the Credit Information Act. Lastly, the information communication sector is subject to the Framework Act on Electronic Documents and Transactions, the Act on the Protection, Use, etc, of Location Information (the Location Information Act), the Network Act and the Protection of Communications Secrets Act.

8 PII formats

What forms of PII are covered by the law?

PII under the PIPA means information regarding a living person such as the name, resident registration number or image that can identify such living person. Even if a certain piece of information cannot, by itself, identify a person, if the information can be easily combined with other information to identify a person, such information is also deemed to be PII.

There is no limit as to the format or formality of the PII.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The PII protection laws of Korea do not explicitly deal with extraterritorial application. The position of the Korean government, however, is that foreigners or foreign corporations that process PII of Koreans should be subject to the PII protection laws of Korea.

10 Covered uses of PII

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

Under the PIPA, 'processing' means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, retrieval, output, correction, recovery, use, provision, disclosure and destruction of PII and other similar activities. The PIPA does not distinguish between those that control or own PII and those that provide PII processing services to owners. Rather, a single concept or term of 'PII processor' is used for a party (such as a public institution, legal person, organisation or individual) that processes personal information directly or indirectly to operate personal information files for official or business purposes.

Although the PIPA does not impose different duties on controllers or processors, a higher level of PII protection duties are imposed on governmental agencies compared to the private sector. Such obligations include the duties to:

- disclose the registration of PII files;
- conduct privacy impact assessments;
- grant the data subject the right to access PII; and
- participate in dispute resolution procedures.

Legitimate processing of PII

11 Legitimate processing – grounds

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

As a matter of principle, PII processing is permitted only with the consent of the data subject. However, PII processing without consent is possible for certain exceptional or inevitable cases, such as cases in which:

- statutory exceptions are provided;
- it is inevitable for compliance with the law;
- it is inevitable for governmental agencies to conduct their statutory duties; or
- it is inevitable for executing and performing contracts with the data subject.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Under the PIPA, more stringent rules apply to:

- sensitive information (such as ideology, beliefs, trade union or political party membership, political opinion, health, sexual life or other type of information that could substantially impair the data subject's privacy); and
- personal identification information (such as resident registration number, passport number, driver's licence number or foreigner registration number).

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Under the PIPA, if the PII being processed by the PII processor is collected from someone other than the data subject, the PII processor must notify the data subject of the following information immediately upon the request of the data subject:

- the source of the PII collection;
- the purpose of the PII processing; and
- the right of the data subject to request the PII processor to suspend processing of the data subject's PII.

14 Exemption from notification

When is notice not required?

Notice is not required in the case of exceptional circumstances, such as a threat to life, the risk of bodily harm or the substantial impairment of rights regarding another person's property or other interest.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

In the event the PII processor intends to use PII for marketing purposes, separate consent for such use must be obtained from the data subject.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Under the PIPA, a PII processor must ensure the accuracy, completeness and currency of the PII to the extent required for the purpose of the PII processing.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

When it becomes no longer necessary to retain PII due to the expiry of the PII holding period or the expiry or completion of the purpose of the PII processing, then the PII must be destroyed.

The holding period for PII is determined by the sector-specific laws. For example, the Act on the Consumer Protection in Electronic Commerce, etc, states that information on:

- expression and advertising should be stored for six months;
- contracts and retraction of applications should be stored for five years;
- payment and provision of goods should be stored for five years; and
- consumer complaints and dispute resolution should be stored for three years.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

A PII processor can only use PII for the purpose for which the PII was collected. It is illegal for a PII processor to use the PII beyond the purpose of collection. Accordingly, it can be viewed that the finality principle has been adopted.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

In principle, a PII processor can only use PII for the purpose for which the PII was collected. Although there are exceptions that allow PII processing without consent (such as statutory exceptions, inevitable for compliance with law, inevitable for governmental entities to conduct their statutory duties and inevitable for executing and performing contracts with the data subject), it is difficult to view the use of PII under such exceptions as a new purpose.

Security

20 Security obligations

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

A PII processor is required to implement physical, technical and organisational measures to procure security pursuant to the Enforcement Decree of the PIPA, including the establishment of internal controls and the maintenance of access records in order to prevent loss, theft, leakage, falsification, alteration or impairment of PII.

21 Notification of data breach

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 PIPA, once the PII processor finds out that PII has been leaked, the PII processor must notify, without delay, the data subject of the following:

- the type of PII leaked;
- the timing and account of the leakage;
- the actions that the data subject can take to minimise the damages resulting from the PII leakage;
- the remedial measures being taken by the PII processor and the procedures for compensation for damages; and
- the contact information of the division where the data subject can file for damages.

Further, in the event the PII leakage exceeds the scale prescribed under the Enforcement Decree of the PIPA, the PII processor must notify, without delay, the result of the remedial measures and data subject notification to the Minister of the Ministry of Interior and Safety or other professional agency set forth in the Enforcement Decree of the PIPA.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

A PII processor has the obligation to designate a PII protection officer (often called the data protection officer or DPO) who oversees, and is in charge of, activities related to PII processing. The duties of the DPO include the following:

- the establishment and implementation of PII protection plans;
- the periodical review and improvement of PII processing status and practice;
- the handling of complaints and compensation for damages arising from PII processing;
- the establishment of internal control systems to prevent leakage, misuse and abuse of PII;
- the establishment and implementation of PII protection education plans;
- the protection, control and supervision of PII files; and
- other activities prescribed in the Enforcement Decree of the PIPA for the proper processing of PII.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The obligation to maintain internal records is set out in sector-specific PII protection laws. For example, under the Credit Information Act, credit information companies are required to maintain the following information for three years:

- the name and address of the customer and the name and address of the entity whom the PII was provided to or exchanged with;
- the details of the workscope requested by the customer and the date thereof; and
- the processing details of the requested workscope and the date and details of the credit information provided.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Heads of governmental agencies have the obligation to conduct a privacy impact assessment that analyses the causes and suggests improvements if there is a risk of infringement of PII arising from the management of PII files pursuant to the standards prescribed under the Enforcement Decree of the PIPA.

Additionally, electronic communication business operators and information providers or intermediaries using the electronic communication services provided by electronic communication business operators are required to obtain certification of their overall systems, including the physical, technical and organisational measures in order to ensure the security and reliability of the information communication network.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There are no general obligations that require PII processors to register or file a report with the supervisory authorities. However, for certain specific industries, registration with, or permits from, the relevant supervisory authority is required.

Under the PIPA, governmental agencies that operate PII files must register certain matters regarding the PII files with the Minister of the Ministry of Interior and Safety.

Under the Location Information Act, a permit from the Korea Communications Commission is required to provide location-based services, and the following information is required to be submitted to obtain the permit: the company name, the address of the main office, a description and type of the location-based service and major business facilities including the location information system. On the other hand, any location-based service that does not deal with personal location information can file a report with the Korea Communications Commission pursuant to the Enforcement Decree of the Location Information Act.

Under the Credit Information Act, a permit from the Financial Services Commission is required to conduct a business that deals with credit information, such as a credit rating business, credit investigation business or debt collection business.

26 Formalities

What are the formalities for registration?

With respect to a location-based service, the procedures for obtaining the requisite permit or filing a report is set forth in the Enforcement

Decree to the Location Information Act. No fees are required to be paid to the Korea Communications Commission with respect to the permit or filing.

For credit information businesses, the procedures for obtaining the requisite permit are set forth in the Enforcement Decree to the Credit Information Act. There are no fees to be paid to the Financial Services Commission for obtaining such a permit.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Any location-based service that has not obtained the requisite permit or filed the relevant report will be subject to criminal penalties. Likewise, conducting any credit information business without the requisite permit will be subject to criminal penalties.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

With respect to a location-based service that deals with personal location information, the following criteria will be comprehensively reviewed in determining the issuance of the permit:

- the feasibility of the location-based service plan;
- technical and organisational measures for the protection of personal location information;
- adequacy of the size of facilities regarding the location-based service;
- financial and technical capacity; and
- other matters necessary for conducting a location-based service.

29 Public access

Is the register publicly available? How can it be accessed?

Information on any location-based service or credit information business that has received a permit is publicly available. Information can be accessed through the Korea Communications Commission and the Financial Services Commission.

30 Effect of registration

Does an entry on the register have any specific legal effect?

As registration or filings are not required in general for PII processors in Korea, special legal effects do not exist.

31 Other transparency duties

Are there any other public transparency duties?

Under the PIPA, a PII processor has the obligation to disclose the terms and conditions of its PII processing, such as its PII processing policy. Further, a PII processor must ensure protection of the data subject's rights, such as the data subject's right to access PII.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the PIPA, in order for the PII processor to disclose PII to a third party (including sharing of PII), consent from the data subject is required. Conversely, in order to delegate PII processing to a third party, the consent of the data subject is not required. The rationale behind this dichotomy is that the provision of PII to third parties is for the benefit of the third-party recipient, whereas the delegation of PII processing is for the benefit of the PII processor.

On the other hand, under the Network Act, an information communication service provider is required to notify, and obtain the consent of, the data subject for both the provision of PII to third parties and the delegation of PII processing. Exceptions to the consent requirement are available where the delegation by the information communication network provider is necessary for the performance of the contract on the provision of information communication services and the furtherance of the user's convenience, as long as the other relevant conditions under the Network Act have been satisfied.

Update and trends

The increase in the collection, use and storage of PII through newly emerging technologies of the Fourth Industrial Revolution has given rise to wide discussions on striking a balance between privacy and technological advancement. Recent developments include the amendment of the Location Information Act, which has relaxed the requirements for Location of Things (LOT) businesses. The amendment to the Location Information Act allows LOT businesses to file a report with the Korea Communications Commission instead of obtaining a permit.

In the finance sector, the relaxation of PII regulations is being discussed by regulators to promote further use of cloud computing in the sector.The protection of PII in crypto-currency exchanges is also a hot topic, as certain crypto-currency exchanges have been vulnerable to cybersecurity attacks. Given the ubiquitous nature of these technologies, the discussions inevitably involve international data protection measures. With the adoption of the General Data Protection Regulation in the EU, many Korean companies with a global presence are updating their privacy policies to comply with the GDPR.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Under the PIPA, when PII is being transferred to another party due to a merger or business transfer, the PII processor is required to notify the data subject in advance of such transfer, together with the relevant information pursuant to the procedures set out in the Enforcement Decree of the PIPA. The Network Act has similar restrictions.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Under the PIPA, in order to provide PII to a third party outside Korea, the following information needs to be notified to the data subject and consent must be obtained for such transfer:

- the recipient of PII;
- the recipient's purpose for using PII;
- the type of PII being provided;
- the period of storage and use of PII by the recipient; and
- the right of the data subject to refuse consent to transfer and, in the event there are any disadvantages arising from such refusal, the details of such disadvantage.

A PII processor cannot enter into a contract for overseas transfer of PII in violation of these restrictions under the PIPA. Note, however, that no consent is required when PII is being provided to a third party outside of Korea for the purpose of delegating PII processing.

Under the Network Act, an information communication service provider must obtain consent both for the provision of information to a third party and for the delegation of PII processing to a third party. Exceptions to the consent requirement are available where the delegation by the information communication network provider is necessary for the performance of the contract on the provision of information communication services and the furtherance of the user's convenience, as long as the other relevant conditions under the Network Act have been satisfied.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Approval or authorisation from a supervisory authority is not required for cross-border transfer of PII.

Notwithstanding, the government can require an information communication service provider to adopt the following measures with respect to the processing of information related to national security and policies or information regarding advanced technology or devices developed in Korea:

- the establishment of systematic and technical measures to prevent the illegitimate use of the information communication network;
- systematic and technical measures to prevent the unlawful destruction or manipulation of information; and
- measures to prevent the leakage of material information acquired during the information communication service provider's processing of information.

36 Further transfer

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.

Rights of individuals

37 Access

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

Under the PIPA, a data subject can request a PII processor for access to the PII being processed. Upon such request from the data subject, the PII processor must allow the data subject to access his or her PII within the time-frame set forth in the Enforcement Decree of the PIPA. If there is any justifiable cause for delay in granting the data subject access, the PII processor can extend the time-frame by notifying the data subject of such extension and the relevant cause. Once the cause no longer exists, the PII processor must grant access to the data subject without delay.

The PII processor can refuse or limit the data subject's access in the event there are:

- statutory prohibitions or restrictions on access;
- potential threat to life or risk of bodily harm; or
- potential impairment of property or other rights of another person.

In such cases, the PII processor must notify the data subject of the reason for the refusal or limitation of access.

38 Other rights

Do individuals have other substantive rights?

Under the PIPA, an individual can require a PII processor to correct or delete his or her PII once the data subject has accessed and reviewed his or her PII. Further, the data subject can require the PII processor to suspend processing of his or her PII.

39 Compensation

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 PIPA, a data subject can seek monetary damages or compensation if the damages incurred by the data subject were due to the violation of the PIPA by the PII processor. In such cases, the PII processor will be liable unless it can prove that there was no intentional misconduct or negligence on the part of the PII processor. If the data subject incurred damages caused by the loss, theft, leakage, falsification, alteration or impairment of PII arising from the intentional misconduct or negligence of the PII processor, the court can order payment of damages up to three times the amount of the damages incurred.

40 Enforcement

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

Both. The rights of data subjects under the PIPA can be exercised through litigation in court or by filing a request for corrective orders with regards to a PII processor's infringement of the data subject's legitimate rights.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No further provisions.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Data subjects can appeal against unlawful orders of the supervisory authorities to the courts.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

There are no specific statutory provisions that deal with cookies or equivalent technology. Nonetheless, cookies can be viewed as PII in certain circumstances.

JIPYONG JIPYONG LLC

Seung Soo Choi **sschoi@jipyong.com**
Seungmin Jasmine Jung **smjung@jipyong.com**

10F, KT&G Seodaemun Tower
60 Chungjeong-ro
Seodaemun-gu
Seoul 03740
Korea

Tel: +82 2 6200 1759/+82 2 6200 1712
Fax: +82 2 6200 0812
www.jipyong.com

Under the Network Act, an information communication service provider is required to include in its PII processing policy terms regarding the installation, operation and rejection of devices that automatically collect PII, such as internet connection record files. Such a PII processing policy should be disclosed to its users in an easily accessible manner according to the requirements of the Enforcement Decree to the Network Act.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Under the Network Act, in order to distribute marketing information for commercial purposes through electronic transmission, the express prior consent of the recipient is required. In the following cases, however, such consent requirement is waived:

- a party that has collected the recipient's contact information through transactions regarding certain goods sends the recipient marketing information for commercial purposes regarding the same type of goods; and
- a telemarketer under the Act on Door-to-Door Sales, etc, verbally notifies the recipient where his or her PII was collected and makes solicitations over the telephone.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

The Act on the Development of Cloud Computing and Protection of Its Users (the Cloud Computing Act) was enacted in 2015 and is currently in effect. The principles of the PIPA and the Network Act as well as sector-specific laws may also apply to cloud computing service providers.

Under the Cloud Computing Act, a cloud computing service provider must endeavour to enhance the quality, performance and data protection levels of its cloud computing service. The Minister of the Ministry of Science and ICT has the authority to set out the standards for quality, performance and data protection (including physical, technical and organisational measures) and issue a recommendation to cloud service providers to comply with such standards.

Under the Cloud Computing Act, a cloud service provider cannot disclose a user's information to a third party nor use the user's information for purposes other than providing cloud computing services without the user's consent, unless a court order or subpoena has been issued by a judge. The user can require the cloud computing service provider to inform the user of the country in which the user's information is stored.

Lithuania

Laimonas Marcinkevičius
Juridicon Law Firm

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The European Parliament and the Council released regulation 2016/679 (the GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, which came into force on 25 May 2018. Regulation 2016/679 is a direct application document and applies in all EU member states from this date. In Lithuania, certain aspects will also be discussed in the new version of the Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter referred to as LPPDL). The Ministry of Justice of the Republic of Lithuania has submitted a draft of the LPPDL to institutions and the public. It was expected that the new version of the LPPDL would come into force on 25 May 2018, but unfortunately it has not come into force yet. At the time of writing, data protection in Lithuania is governed by the LPPDL, which is substantially based on the European Union Data Privacy Directive 95/46/EC. The answers below are based on the current version of the LPPDL.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Lithuanian data protection authority is the State Data Protection Inspectorate (SDPI). The SDPI has the right to:

- obtain access, subject to a prior notice in writing, or without a prior notice where the lawfulness of the processing of personal data is to be checked in response to a complaint, to premises of the person being checked (including the premises rented or used on other grounds), or to the territory where the documents and equipment related with the processing of the personal data are kept. Access to the territory, buildings and premises of a legal person (including the buildings and premises rented or used on any other grounds) shall be permitted only during office hours of the legal person being checked upon presenting a certificate of a civil servant. Access to residential premises (including premises leased or used on any other basis) of a natural person being checked, where documents and facilities related with the personal data processing are kept, shall be permitted only upon producing a court order warranting entry into the residential premises;
- obtain, free of charge, from state and municipal institutions and agencies, and other legal and natural persons the entire necessary information, copies and transcripts of documents, copies of data and access to all data and documents necessary for the discharge of its functions of the supervision of personal data processing;
- make recommendations and give instructions to the data controller on personal data processing and protection issues;
- draw up records of administrative offences in accordance with the procedure laid down in law;
- use photo, video and audio recording equipment in gathering evidence in the course of checking the lawfulness of personal data processing; and
- take part in legal proceedings over violations of the provisions of international and national law on personal data protection.

3 Legal obligations of data protection authority

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

One of the SDPI functions established in the LPPDL is to cooperate with foreign institutions in charge of the protection of personal data, European Union institutions, agencies and international organisations, and take part in their activities.

4 Breaches of data protection

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

The breaches of rules stipulated by the LPPDL may result in administrative liability. The SDPI has the right to draw up records of administrative offences. Breaches may be fined.

The illegal collection of information about a person's private life or the disclosure and use of this type of information may also result in criminal liability. These breaches are punished by imprisonment for a maximum period of three years, arrest, restriction of liberty, a fine or community service. Offences such as disclosure and use of information about a person's private life are prosecuted only if a formal complaint has been filed by the affected data subject or his or her legitimate representative or upon request of the prosecutor.

Moreover, according to the LPPDL, any person who has sustained damage as a result of unlawful processing of personal data or any other acts (omissions) by the data controller, the data processor or other persons violating the provisions of this law shall be entitled to claim compensation for pecuniary and non-pecuniary damage caused to him or her. The extent of pecuniary and non-pecuniary damage shall be determined by a court.

Scope

5 Exempt sectors and institutions

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

The LPPDL provides for certain exceptions (there are entities or areas of activity to which it does not apply). The LPPDL does not apply if personal data is processed by a natural person only for his or her personal needs not related to business or profession, and also does not apply to the processing of personal data of deceased persons. When personal data is processed for the purposes of state security or defence, the LPPDL shall apply to the extent that other laws do not provide otherwise.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The LPPDL does not wholly cover the interception of communications, electronic marketing or monitoring and surveillance of individuals. Relevant laws in this regard are: the Law on Electronic Communications of the Republic of Lithuania and the Law on Cybersecurity of the Republic of Lithuania.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

The Law on Mass Media of the Republic of Lithuania contains rules that apply to the protection of personal data that is used for mass media purposes. The Civil Code of the Republic of Lithuania and other healthcare acts contain special rules for the protection of information about patients' health. The Law on Legal Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters contains regulations on personal data processing during police and judicial cooperation in criminal matters. The Republic of Lithuania Labour Code provides an obligation for employers to approve and inform employees about information and communication technology use, and employee monitoring and control procedures in the workplace.

8 PII formats

What forms of PII are covered by the law?

The LPPDL regulates relations arising in the course of the processing of personal data by automatic means, and during the processing of personal data by other than automatic means in filing systems: lists, card indexes, files, codes, etc.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The LPPDL is applicable when:

- personal data is processed by a data controller established and operating in the territory of Lithuania, as a part of activities thereof. Where personal data is processed by a branch office or a representative office of a data controller of a member state of the European Union or another state of the European Economic Area, established and operating in the Republic of Lithuania, such a branch office or representative office shall be bound by the provisions of the law applicable to the data controller;
- personal data is processed by a data controller established in a territory other than the Republic of Lithuania, but which is bound by the laws of the Republic of Lithuania by virtue of international public law (including diplomatic missions and consular posts);
- personal data is processed by a data controller established and operating in a country that is not a member state of the European Union or another state of the European Economic Area (hereinafter referred to as a third country), where the data controller uses personal data processing means established in the Republic of Lithuania, with the exception of cases where such means are used only for the transit of data through the territory of the Republic of Lithuania, the European Union or another state of the European Economic Area. In the case laid down in this subparagraph, the data controller must have a representative; that is, an established branch office or a representative office in the Republic of Lithuania, which shall be bound by the provisions of the law applicable to the data controller.

10 Covered uses of PII

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

Essentially all processing or use of PII is covered by the LPPDL; other laws provide for more detailed provisions for specific sectors and types of organisation or some areas of activity (see questions 5 and 6). There is also a distinction between the data controller (a legal or a natural person who alone or jointly with others determines the purposes and means of processing personal data) and the data processor (a legal or a natural person other than an employee of the data controller, processing personal data on behalf of the data controller).

Legitimate processing of PII

11 Legitimate processing – grounds

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

Lithuanian legal regulation requires that the holding of PII has specific legal ground for the processing of personal data. According to the LPPDL, personal data may be processed if:

- the data subject has given his or her consent;
- a contract to which the data subject is party is being concluded or performed;
- it is a legal obligation of the data controller under laws to process personal data;
- processing is necessary in order to protect vital interests of the data subject;
- processing is necessary for the exercise of official authority vested by laws and other legal acts in state and municipal institutions, agencies, enterprises or a third party to whom personal data is disclosed; or
- processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data is disclosed, unless such interests are overridden by the interests of the data subject.

For special categories of personal data (data concerning the racial or ethnic origin of a person, his or her political opinions or religious, philosophical or other beliefs, membership of trade unions, and his or her health, sexual life and criminal convictions), the LPPDL stipulates stricter grounds.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The processing of special categories of personal data (data concerning the racial or ethnic origin of a person, his or her political opinions or religious, philosophical or other beliefs, membership of trade unions, and his or her health, sexual life and criminal convictions) is generally prohibited, unless special conditions are met. According to the LPPDL, the processing of such personal data is allowed if:

- the data subject has given his or her consent;
- such processing is necessary for the purposes of employment or civil service while exercising the rights and fulfilling obligations of the data controller in the field of labour law in the cases laid down in law;
- it is necessary to protect the vital interests of the data subject or of any other person, where the data subject is unable to give his or her consent due to a physical disability or legal incapacity;
- the processing of personal data is carried out for political, philosophical or religious purposes or purposes concerning trade unions by a foundation, association or any other non-profit organisation as part of its activities, on condition that the personal data processed concerns solely the members of such organisation or to other persons who regularly participate in such organisation in connection with its purposes. Such personal data may not be disclosed to a third party without the data subject's consent;

- the personal data has been made public by the data subject;
- the data is necessary, in the cases laid down in law, in order to prevent and investigate criminal or other illegal activities;
- the data is necessary for a court hearing; or
- it is a legal obligation of the data controller under laws to process such data.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The LPPDL requires owners of PII to notify individuals about the fact that their data is being processed. In cases where personal data is collected from the data subject, the controller is obliged to provide the data subject from whom the data is collected with the following information:

- the identity and permanent place of residence of the data controller and his or her representative, if any (where the data controller or its representative is a natural person), or indicate the name, code and address of the registered office (where the data controller or its representative is a legal person);
- the purposes of processing the data subject's personal data; and
- other additional information (the recipient and the purposes of disclosure of the data subject's personal data; the personal data that the data subject must provide and the consequences of his or her failure to provide the data; the right of the data subject to have access to his or her personal data; and the right to request rectification of incorrect, incomplete and inaccurate personal data) to the extent that is necessary for ensuring the fair processing of personal data without infringing upon the data subject's rights.

According to the LPPDL, in cases where the data controller obtains personal data not from a data subject, he or she must inform the data subject thereof before commencing the processing of personal data or, if he or she intends to disclose the data to third parties, he or she must inform the data subject thereof at the latest when the data is first disclosed, except in cases where laws or other legal acts determine a procedure for collecting or disclosing such data and data recipients. In such cases, the data controller must provide the data subject with all the information that is listed in the bullet points above.

When the data controller collects or intends to collect personal data from the data subject and processes or intends to process the data for the purposes of direct marketing, before disclosing the subject's data he or she must inform the data subject about the recipient of his or her personal data and the purposes for which his or her personal data will be disclosed.

14 Exemption from notification

When is notice not required?

Notice is not required if the individual is already acquainted with such information. In a case where the personal data has not been obtained from the data subject, the controller is not obliged to provide the data subject with the proper notice if personal data is processed for statistical, historical or scientific research purposes; where the disclosure of such information is impossible or too complicated (owing to a large number of data recipients, the outdated character of the data or excessively large expenses); or where the procedure for collecting and disclosing of data is laid down by law. The data controller must duly notify the SDPI thereof in accordance with the procedure laid down in the LPPDL. The SDPI must carry out a prior check.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The owners of PII are obliged to ensure individuals exercise their statutory rights. The data subject has the right to access his or her personal data and to be informed of how it is processed; to request rectification or destruction of his or her personal data or suspension of further processing of his or her personal data, with the exception of storage, where the data is processed in violation of the provisions of the LPPDL and other laws; and to object against the processing of his or her personal data.

The data subject has the right, upon presenting to the data controller or the data processor a document certifying his or her identity or upon confirming his or her identity in accordance with the procedure laid down by legal acts or by means of electronic communications that permit a person's identification, to obtain information on the sources and type of personal data that has been collected, the purpose of its processing and the data recipients to whom the data is disclosed or has been disclosed within the past year.

Where a data subject, after familiarising himself or herself with his or her own personal data, finds that the data is incorrect, incomplete or inaccurate and applies to the data controller, the latter must check the personal data concerned without delay and, at a written request of the data subject submitted in person, by post or by means of electronic communications, rectify the incorrect, incomplete and inaccurate personal data and suspend the processing of such personal data, except storage, without delay.

Where a data subject, after familiarising himself or herself with his or her own personal data, finds that the data is processed unlawfully and unfairly and applies to the data controller, the latter must check without delay and free of charge the lawfulness and fairness of the processing of personal data and, at a written request of the data subject, destroy the personal data collected unlawfully and unfairly or suspend processing of such personal data, except storage, without delay.

A data subject has the right to object to the processing of his or her personal data without providing reasons for such objection where the data is or is intended to be processed for the purposes of direct marketing or for the purposes of a social and public opinion survey.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

According to the LPPDL, the data controller must ensure that personal data is processed accurately, fairly and lawfully. Personal data must also be accurate and, where necessary for the purposes of personal data processing, kept up to date; inaccurate or incomplete data must be rectified, supplemented, erased or its further processing must be suspended. Personal data must also be identical, adequate and not excessive in relation to the purposes for which it is collected and further processed.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The amount of PII that may be held is mentioned in question 16: personal data must be identical, adequate and not excessive in relation to the purposes for which it is collected and further processed. Regarding the length of time the data may be held, there are no particular provisions regulating that matter. According to the LPPDL, personal data shall not be stored longer than it is necessary for data processing purposes. Personal data must be destroyed when it is no longer needed for processing purposes, with the exception of data that must be transferred to state archives in the cases laid down in law.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The LPPDL states that the data controller must ensure that personal data is collected for specified and legitimate purposes and is not subsequently processed for purposes incompatible with the purposes determined before the personal data concerned is collected.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The processing of personal data for a purpose other than that intended at the time of data collection is allowed for statistical, historical or

scientific research purposes only in the cases laid down in law, provided that adequate data protection measures are laid down in law.

Security

20 Security obligations

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

According to the LPPDL, the data controller and the data processor must implement the appropriate organisational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. These measures must ensure:

- a level of security appropriate in respect of the nature of the personal data to be protected (according to legal regulation there are three security levels, from one to three. To ensure these security levels in legal regulation there are special requirements for each one, which contain, for example, the requirement to produce a security policy and a computer system management instruction used for personal data processing; the requirement that, in cases where a password is used for user authentication in the computer system used for data processing, the password shall consist of at least eight characters, including upper- and lower-case letters, numbers and special characters); and
- the risks represented by the processing must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc).

21 Notification of data breach

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 came into force, the LPPDL did not provide a general obligation of notification of a security breach. Only when the processing of personal data was rectified, destroyed or suspended at the request of the data subject must the data controller, without delay, inform data recipients, unless the disclosure of such information proves impossible or involves a disproportionate effort (owing to a large number of data subjects, the period covered by the data or excessively large expenses). In this case, the SDPI must be notified without delay. According to the Law on Electronic Communications of the Republic of Lithuania, a company that is a provider of public communications networks or publicly available electronic communications services in the case of a security breach is obligated to report this violation to the SDPI within 24 hours.

After the GDPR came into force, this regulation's obligations are applicable. In order to assist data controllers in their obligation to report personal data breaches, the SDPI has prepared the Recommended Form of Reporting on Personal Data Security Violations.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The appointment of a data protection officer (a person or unit) is voluntary. If a data protection officer is appointed, the owner of PII must notify the SDPI. A person or unit responsible for data protection shall:

- make public the actions of personal data processing carried out by the data controller in accordance with the procedure established by the government;
- supervise as to whether personal data is processed in compliance with the provisions of the LPPDL and other legal acts regulating data protection;
- initiate the preparation of notifications of the existence of the circumstances specified in paragraph 1 of article 33 of the LPPDL to the SDPI;
- monitor the processing of personal data carried out by the data controller's employees;
- present proposals, findings to the data controller regarding determination of data protection and data processing measures and supervise the implementation and use of these measures;
- undertake, without delay, measures to eliminate any violations in the processing of personal data;
- instruct employees authorised to process personal data on the provisions of this law and other legal acts regulating personal data protection;
- initiate the preparation of applications to the SDPI on the issues of the processing and protection of personal data;
- assist data subjects in exercising their rights; and
- notify the SDPI in writing upon establishing that the data controller processes personal data violating the provisions of the LPPDL and other legal acts regulating data protection and refuses to rectify these violations.

For companies with more than 50 employees, there is a requirement set in the Republic of Lithuania Labour Code to confirm and publish data protection and privacy policies.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

According to the LPPDL, data subjects have a right to request detailed information about what data of theirs is processed and how it is processed (see question 15). The owners of PII have to comply with all such requests every time. Therefore, the owners are subject to various data storage duties, detailed in legal regulation. When authorising the data processor to process personal data, the data controller shall establish that personal data is processed only in accordance with the data controller's instructions.

24 New processing regulations

Are there any obligations in relation to new processing operations?

According to LPPDL the data controller and the processor must implement appropriate organisational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. The SDPI has submitted a draft of list of operations for which a privacy impact assessment is needed.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

According to the LPPDL, personal data may be processed by automatic means only when the data controller or its representative (in this context data controller representative is an established branch office or a representative office in the Republic of Lithuania which shall be bound by the provisions of the LPPDL applicable to the data controller, when personal data is processed by a data controller established and operating in country that is not a member state of the European Union or another state of the European Economic Area) notifies the SDPI in accordance with the procedure established by the government. The obligation does not apply when personal data is processed:

- for the purposes of internal administration;
- for political, philosophical, religious or trade union-related purposes by a foundation, association or any other non-profit organisation on condition that the personal data processed relates solely to the members of such organisation or to other persons who regularly participate in its activities in connection with the purposes of such organisation;
- in the cases laid down in article 8 of the LPPDL (which states that the processing of personal data by the media for the purpose of providing information to the public, artistic and literary expression shall be supervised by the Inspector of Journalist Ethics); or
- in accordance with the procedure laid down in the Law on State Secrets and Official Secrets.

26 Formalities

What are the formalities for registration?

The form for notification to the SDPI can be submitted directly to the SDPI or via mail or public communications network. There are no fees for notification.

The notification form submitted to the SDPI should contain the following:

- the main information about the controller: name, legal person code, address of its seat, telephone and fax numbers, and email address or, if the data controller is a natural person, his or her name, personal code and place of residence and place of data processing, telephone and fax numbers, and email address;
- the purpose of processing the data;
- personal data sources;
- information relating to a possible data transfer to a third country (the aim of the processing data, list of the data, the state or group of states or groups);
- the data subject group or groups, distinguished by their characteristics (land owners, retirees, debtors and others), and the related list of personal data;
- the data recipient or recipients of the data group or groups, distinguished by their characteristics (debt collection companies, banks and others), for which data controllers provide personal data;
- personal data storage period; and
- the list of the data controllers and their representatives (if they have representatives).

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

A person who, regardless of the obligation laid down in the LPPDL, fails to notify the SDPI about processing personal data, is liable to a fine.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The SDPI may refuse to register a data controller if:

- the requirements specified in question 26 have not been fulfilled;
- the processing of personal data does not comply with the requirements in legislation governing the processing of personal data; or
- the data controller reported on the processing of personal data, but according to the LPPDL this obligation does not apply (see exemptions of this obligation in question 25).

29 Public access

Is the register publicly available? How can it be accessed?

The register is publicly available and can be accessed online (www.ada.lt/go.php/lit/img/5).

30 Effect of registration

Does an entry on the register have any specific legal effect?

No specific legal effect is connected with entering the register. The register is for information purposes: to give the SDPI details on the data processing and to provide transparency for the affected individuals and the public.

31 Other transparency duties

Are there any other public transparency duties?

Neither the LPPDL nor the draft of the new version of the LPPDL establish any transparency duties other than those established in the GDPR.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

According to the LPPDL, personal data shall be disclosed under a personal data disclosure contract between the data controller and the data recipient in the case of a multiple disclosure or in response to a request from the data recipient in the case of a single disclosure. The contract must specify the purpose for which personal data will be used, the legal basis for disclosure and receipt, the conditions, the procedure of use and the extent of personal data that is disclosed. The request must specify the purpose for which personal data will be used, the legal basis for disclosure and receipt and the extent of personal data requested.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

The LPPDL provides specific requirements in the scope of the agreement that the data controller needs to conclude with the data processor (see question 32).

Under the LPPDL, where personal data is processed by automatic means and appropriate measures ensuring data security are applied, in providing personal data under a personal data disclosure contract between the data controller and the data recipient, priority must be given to disclosure of the data by automatic means, and when disclosing personal data at the request of the data recipient, to disclosure of data by means of electronic communications.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

According to the LPPDL, the transfer of personal data to data recipients in third countries (ie, outside of the EEA) shall be subject to an authorisation from the SDPI, except in the cases referred to in the LPPDL. Authorisation shall be granted provided that there is an adequate level of legal protection of personal data in these countries. The level of legal protection of personal data shall be assessed by considering all circumstances related to the transfer of data, particularly the laws and other legal acts or acts prepared by the data controller on legal protection of personal data in force in the third country of destination, the nature of the data to be transferred, the methods, purposes and duration of the data processing and safeguards applicable in the country concerned.

However, without the SDPI's authorisation, it is possible to transfer personal data to a third country or to an international law enforcement organisation only if:

- the data subject has given his or her consent for the transfer of the personal data;
- the transfer of personal data is necessary for the conclusion or performance of a contract between the data controller and a third party in the interests of the data subject;
- the transfer of personal data is necessary for the performance of a contract between the data controller and the data subject or for the implementation of pre-contractual measures to be taken in response to the data subject's request;
- the transfer of personal data is necessary (or required by law) for important public interests or for the purpose of legal proceedings;
- the transfer is necessary for the protection of the data subject's vital interests;
- the transfer is necessary for the prevention or investigation of criminal offences; and
- personal data is transferred from a public data file in accordance with the procedure laid down in laws and other legal acts.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

The duty to get authorisation from SDPI applies to the extent as outlined in question 34. According to the LPPDL, personal data shall be transferred to data recipients in the member states of the European Union or other countries of the European Economic Area under the

same conditions and in accordance with the same procedure as is applicable to data recipients in the Republic of Lithuania.

36 Further transfer

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 data transfers to third countries (ie, outside of the EEA) apply to every form of data transfer.

Rights of individuals

37 Access

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

The right for the data subject to access personal information held by PII owners is set in the LPPDL. Under the legal regulation, the data subject has the right, upon presenting to the data controller or the data processor a document certifying his or her identity or upon confirming his or her identity in accordance with the procedure laid down by legal acts or by means of electronic communications that permit a person's identification, to obtain information on the sources and type of personal data that has been collected, the purpose of its processing and the data recipients to whom the data is disclosed or has been disclosed during the past year.

There is, however, a limit to the right of access: the data controller must provide the data subject with the conditions for exercising the rights laid down in the LPPDL, with the exception of cases laid down in law when it is necessary to ensure:

- the security or defence of the state;
- public order and the prevention, investigation, detection or prosecution of criminal offences;
- important economic or financial interests of the state;
- the prevention, investigation and detection of violations of official or professional ethics; and
- the protection of the rights and freedoms of the data subject or other persons.

The data controller must justify a refusal to grant the request of the data subject to exercise the rights granted to the data subject by the LPPDL. Moreover, the data controller shall disclose such data to the data subject free of charge once per calendar year. When such data is disclosed for a fee, the amount of the fee may not exceed the cost of disclosure of the data. The procedure governing the fee for disclosure of data shall be determined by the government.

38 Other rights

Do individuals have other substantive rights?

According to the LPPDL, data subjects whose data is being processed have the right not only to obtain information but also:

- to know (be informed) about the processing of his or her personal data (see question 13);
- to request the rectification or destruction of the personal data or suspension of further processing of the personal data, with the exception of storage, where the data is processed in violation of the provisions of this law and other laws (see question 15); and
- to object against the processing of his or her personal data (see question 15).

39 Compensation

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 LPPDL, any person who has sustained damage as a result of unlawful processing of personal data or any other acts (omissions) by the data controller, the data processor or other persons violating the provisions of the law shall be entitled to claim compensation for pecuniary and non-pecuniary damage caused. The extent of pecuniary and non-pecuniary damage shall be determined by a court.

Update and trends

According to various surveys, there are still many companies (data controllers) in Lithuania that do not comply with the GDPR requirements. In order to assist data controllers, the SDPI publishes guides and other useful material about data protection requirements on its official website. New versions of legislation for data protection are also being prepared.

The Ministry of Justice of the Republic of Lithuania has submitted a draft of the LPPDL to institutions and the public, which has not come into force yet.

The SDPI has submitted the following drafts of documents, which give details on GDPR implementation:

- a draft of list of operations, for which a privacy impact assessment is needed;
- in order to assist data controllers in their obligation to report personal data breach, the Recommended Form of Reporting on Personal Data Security Violations and description of the procedure for informing the SDPI about a personal data breach; and
- a draft of prior consultations (GDPR article 36) procedure.

It is expected that for Lithuanian data controllers, the coming year will be devoted to data protection compliance issues.

40 Enforcement

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

The SDPI is only entitled to control the provisions of the LPPDL and other data privacy regulations. It also can draw up records of administrative offences in accordance with the procedure laid down in law. However, the SDPI is not competent in assigning damages claims against data owners. As mentioned in question 39, the extent of pecuniary and non-pecuniary damage shall be determined by a court.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The main limitations are described above. The LPPDL also includes regulations related to restrictions of video surveillance (for example, video surveillance may be used for the purpose of ensuring public safety, public order and protecting the life, health, property and other rights and freedoms of persons but only in cases when other ways or measures are insufficient or inadequate for the achievement of the above-mentioned purposes, unless they are overridden by the interests of the data subject); and the processing of personal data for an evaluation of solvency and debt management (for example, the data controller may disclose debtors' data on condition that the controller has sent a written reminder to the data subject about a default on obligations and where, within 30 calendar days of the sending (submitting) date of the reminder, the debt is not settled or the deadline for the repayment is not extended; or the data subject does not contest the debt on compelling grounds).

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

According to Lithuanian legal regulations, PII owners can appeal against orders of the SDPI to the administrative courts.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The use of cookies is allowed only on condition that the subscriber or user concerned is provided with clear and comprehensive information about such use in accordance with the procedure and conditions set out in the LPPDL, including information about the purposes of the processing of information, and is offered the right to refuse such processing by the data controller. These provisions shall not prevent technical storage or access for the sole purpose of carrying out or facilitating the transmission of information over an electronic communications network, or as strictly necessary in order to provide an information society service ordered by the subscriber or the actual user of electronic communications services.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Under the LPPDL, personal data may be processed for the purposes of direct marketing (direct marketing shall mean an activity intended for offering goods or services to individuals by post, telephone or any other means and for obtaining their opinion about the offered goods or services) only after the data subject gives his or her consent. The data controller must provide a clear, free-of-charge and easily realisable possibility for the data subject to give or refuse consent for the processing of personal data for the purposes of direct marketing.

On the other hand, the data controller, while rendering services or selling goods in accordance with the procedure and conditions set by the LPPDL, receives contact information (name, surname and address) from data subjects that are its customers may only use this data without a separate data subject's consent for the marketing of its own goods or services or of a similar nature, provided that customers have been given a clear, free-of-charge and easily realisable possibility not to give their consent or refuse giving their consent for the use of this data for the above-mentioned purposes at the time of collection of the data and, if initially the customer has not objected against such use of the data, at the time of each offer.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Lithuanian national law does not regulate cloud computing services.

LAW FIRM
JURIDICON
MARCINKEVIČIUS & PARTNERS

Laimonas Marcinkevičius **laimonas.marcinkevicius@juridicon.lt**

Totorių St. 5–7,
LT-01121 Vilnius,
Lithuania

Tel: +370 5 269 11 00
Fax: +370 5 269 10 10
http://juridicon.lt/en

Malta

Ian Gauci and Michele Tufigno
Gatt Tufigno Gauci Advocates

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

As a member state of the European Union, Malta's data protection laws include the EU's General Data Protection Regulation (2016/679) (GDPR). Chapter 586 of the Laws of Malta, the Data Protection Act (2018), along with its subsidiary legislation, came into force on 28 May 2018, repealing the previous Data Protection Act of 2001.

Malta is also a party to the Convention for the Protection of Individuals regarding the Automatic Processing of Personal Data (ETS.108), which came into force in 2003.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Office of the Information and Data Protection Commissioner, appointed according to article 11 of the Data Protection Act (2018), is the supervisory authority responsible for overseeing the applicability and enforcement of data protection law in accordance with the requirements of the GDPR.

Further to the provisions of the GDPR and the Data Protection Act (2018), the Commissioner shall have the right to carry out investigations in the form of data protection audits and inspections, as well as demand and access personal data and data processing equipment, records and documentation held by data controllers or data processors. The Commissioner may also request the assistance of the executive police to enter and search any premises in the course of investigation. Moreover, when exercising such investigative powers, the Commissioner may ask for additional information from any person deemed to be of interest; lack of cooperation or the provision of false information may lead to criminal prosecution.

3 Legal obligations of data protection authority

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

The Data Protection Act (2018) provides for joint operations with the supervisory authorities of other EU member states. The Act refers to the GDPR in instances when the national supervisory authority is to cooperate with other supervisory counterparts. In such cases, the Commissioner is to confer his or her powers, including investigative ones, to members and staff of the member states' supervisory authorities; the Act (2018) provides that such conferment of powers is to be made under the exercise and in the presence of the Commissioner.

The GDPR envisages that data protection authorities, referred to as supervisory authorities, provide relevant information and give mutual assistance to other supervisory authorities, thus ensuring that the GDPR is implemented in a consistent manner.

4 Breaches of data protection

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

The GDPR provides that administrative fines can be imposed pursuant to its infringement. It is also stipulated that such fines must be effective, proportionate and dissuasive. Supervisory authorities are also instructed to take into consideration several elements when imposing such fines, including but not limited to intent, gravity and degree of cooperation. Different infringements carry different administrative fines.

The Data Protection Act (2018) specifies the administrative fines that can be imposed by the Commissioner by order in writing upon the controller or processor, which fines shall be due to the Commissioner as a civil debt should such persons be found in breach of applicable data protection laws; such fines have not been capped. Fines shall not exceed €25,000 per violation in the case of public authorities or bodies. Moreover, a daily fine can be imposed by the Commissioner for each day on which the violation persists.

With reference to criminal penalties, the Act (2018) stipulates that if a person knowingly provided false information to the Commissioner or else failed to comply with a lawful request made by the Commissioner during an investigation, that person is to be found guilty of a criminal offence and will be liable to a fine running up to €50,000, with a possible term of imprisonment for six months.

Scope

5 Exempt sectors and institutions

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 (2018) provides that certain entities, persons and activities are excluded from the scope of the law and consequently the requirements of the GDPR. In this case the Act (2018) follows the provisions of the GDPR when it comes to exempt sectors and institutions. The processing of personal data for activities falling outside of the scope of Union law are excluded; data protection laws also do not apply when the Government of Malta carries out activities in accordance with the scope of chapter 2 of Title V of the Treaty of the European Union, dealing with common foreign and security policy. Natural persons carrying out personal and household activities are also excluded from the scope of the law. Finally, competent authorities are also excluded from the scope of the law when processing data with the purpose of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties, including the safeguarding against and the prevention of threats to public security.

It is also to be noted that the Act (2018) allows certain derogations to be made when processing personal data for scientific, historical, archiving or official statistical purposes. These derogations are only allowed if the full applicability of the law renders the achievement of the exercises in question impossible or impaired and if the data controller believes that such derogations are necessary. In addition, the

Act provides that the provisions of the GDPR could be further derogated from in order to exercise the right to freedom of expression and information.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Data Protection Act (2018) itself makes no reference to the interception of communications, electronic marketing or monitoring and surveillance of individuals.

Subsidiary Legislation 586.08, titled 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 and implementing Directive (EU) 2016/680 of the European Parliament and of the Council, addresses technical surveillance, in that it is lawful for competent authorities to collect personal data through technical surveillance or through automated means.

Under Maltese law, Chapter 391 of the Laws of Malta, titled the Security Service Act, addresses the interception of communications, which by the definition provided in the same Act includes an array of activities such as surveillance; the act itself makes no reference to the processing of data. On the other hand, the GDPR addresses direct marketing, but does not distinguish between electronic and non-electronic marketing. In cases of direct marketing, the data subject has the right to object to the processing of their data for marketing purposes.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Under Maltese law, apart from the Data Protection Act (2018), there are various subsidiary legislations implementing EU regulation or regulations issued by the Minister responsible for data protection.

- Subsidiary Legislation 586.01, titled Processing of Personal Data (Electronic Communications Sector) Regulations and implementing Directive 2002/52 EU of the European Parliament and Council, addresses the processing of data when providing publicly available electronic communications services in public communications networks in Malta and any other country.
- Subsidiary Legislation 586.06, titled Processing of Personal Data for the Purposes of the General Elections Act and the Local Councils Act Regulations, deals with the processing of data in elections held in accordance with Maltese electoral law.
- Subsidiary Legislation 586.07, titled Processing of Personal Data (Education Sector) Regulations, addresses the processing of data by educational institutions and authorities.
- Subsidiary Legislation 586.10, titled Processing of Data Concerning Health for Insurance Purposes Regulations, adds to the existing data protection law when it comes to processing data for insurance purposes and provides for lawful scenarios in which data can be collected.
- Subsidiary Legislation 586.11, titled Processing of Child's Personal Data in Relation to the Offer of Information Society Services Regulations, provides for the minimum age, currently 13, that minors must have attained for information society services to be able to process the child's data in the absence of parental consent.

8 PII formats

What forms of PII are covered by the law?

The GDPR lays down rules for the protection of natural persons when their personal data is processed and makes no distinction with regard to its form. The Data Protection Act (2018) upholds the same scope of the GDPR in that data protection law applies to the processing of personal data, wholly or partly, either by automated means or otherwise, where such data is processed to form part of a filing system or is intended for such purpose.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The Data Protection Act (2018) mirrors its provisions on the GDPR when defining its territorial scope. The Act is applicable when the processing of data occurs by a data controller (PII owner) or processor in a Maltese establishment. The Act also specifies that processing occurring in a Maltese embassy or in a High Commission situated abroad falls within the scope of the Act. Data controllers or processors not established within the EU are also bound by data protection law if the data subjects being offered goods or services are based in Malta, whether such services or goods are offered for remuneration or free of charge. Data protection law applies if data subjects situated within Malta are being monitored for their behaviour. The provisions of the Act (2018) and the GDPR also apply to data controllers processing data outside of the EU if public international law states that Maltese law is applicable in such circumstances.

10 Covered uses of PII

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

The Data Protection Act (2018), along with the GDPR, provides for the establishment of data subject rights and stipulates when such laws are not applicable and when exclusions and derogations apply. Data protection laws apply solely to natural persons. The aforementioned law and regulation differentiate between the role of the data controller and that of the data processor, imposing different responsibilities upon each party.

Under the GDPR, the data controller must maintain documentation recording data processing undertaken by him or her, which shall be available for consultation at any time. Other measures to be taken by the controller include the implementation of and adherence to data protection policies and codes of conduct, adopting a data protection-by-design approach and ensuring that measures to safeguard data are in place through appropriate technical and organisational structures.

With reference to the data processor, the GDPR provides that personal data should only be processed by the processor following the written instructions provided by the controller. When required, a processor must demonstrate their compliance with the GDPR to the controller and supervisory bodies. Unless the controller gives his or her written consent, a processor cannot engage a sub-processor. The processor is obliged to assist the controller with regard to both data subject requests and compliance. If instructed by the controller, a processor should be able to delete data. Moreover, both parties shall cooperate with supervisory bodies and maintain records of the name and contact details of the processor, controller and DPO; the purpose of data processing; and the types and categories of data and data subjects in their possession, among others.

Legitimate processing of PII

11 Legitimate processing – grounds

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

The Data Protection Act (2018) relies mainly on the provisions of the GDPR, which provide that for the processing of personal data to be lawful, the data subject must either have given his or her explicit consent, or the controller requires such data to be compliant with a legal obligation, or processing is necessary in order to protect the vital interests of the data subjects. Data processing is also legitimate if it is necessary to carry out a task in the public interest or to fulfil the legitimate interests of the controller, unless such a data controller is a public entity, in which case legitimate interest is not considered to be a legal ground for processing.

Where the processing of data is based on the data subject's consent, the controller shall demonstrate that it was the data subject who freely consented to such processing.

When it comes to the processing of personal data belonging to minors, the GDPR speaks about the consent that can be given by minors to offers of information society services. The GDPR provides that if a minor is under the age of 16, processing of the minor's personal data can only be lawful if authorised by the holder of parental authority. In the case of Malta, the age has been lowered to 13, as allowed by the GDPR, for the purposes of subscription or use of information society services.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The GDPR prohibits the processing of special categories of personal data, such as data identifying ethnic origin and political opinions or related to health, among others. However, it lays down certain exceptions whereby special categories of data can be processed in accordance with the law of individual member states. Within the remit of Maltese law, the Act (2018) allows for the processing of identity documents, genetic data, biometric data and data concerning health, provided that such processing follows the specific requirements connected to the processing of such special data.

The Processing of Data Regulations for the Education Sector addresses the processing and use of data by educational institutions and authorities.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The Data Protection Act (2018) makes no specific reference to data controllers (owners of PII) having to notify individuals whose personal data they hold and relies on the GDPR. The latter provides that the data controller may have to communicate with the data subject in cases where the data subject's personal data is rectified or erased. The data controller is also required to notify the data subject should the original processing purposes justifying data collection be changed or expanded and, most importantly, in cases where a data breach has been ascertained and is likely to result in a high risk to the rights and freedoms of the individual. Such notification shall contain a list of the categories and approximate number of data subjects and data records concerned, the contact details of the controller's data protection officer or alternative representative and the likely consequences and measures taken to address and mitigate the breach.

Within the context of Maltese law, it should also be noted that the Restriction of the Data Protection (Obligations and Rights) Regulations refer to scenarios where data controllers may be required to inform data subjects in cases when their rights are restricted, unless such disclosure is prejudicial for the purpose of the restrictions.

14 Exemption from notification

When is notice not required?

The data controller shall not be required to notify the data subject of an ascertained data breach where:

- it has implemented appropriate technical and organisational protection measures to the breached data, defusing the risk to the subject's rights and freedoms;
- the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; and
- individual notification would require a disproportionate effort.

In such a case, the controller shall instead issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The GDPR establishes that controllers must inform data subjects of the purposes and legal grounds for processing, including legitimate interest; information regarding the recipients or categories of recipients of the data subject's data, if any; the intention to transfer the data to a third country or international organisation, if applicable; and the period for which the data will be retained. In cases where processing is based on consent, the data subject shall have the right to withdraw such consent easily, while in cases of processing based upon legitimate interests, the data subject shall have the right to object to such legitimate interests. Furthermore, the GDPR grants the data subject various rights allowing increased control of his or her personal data.

Within the Maltese context, the Restriction of the Data Protection (Obligations and Rights) Regulations provides that when the rights of data subjects are restricted due to the various legitimate reasons provided for by law, the data collected can only be processed for the purpose of its collection, unless the law provides otherwise, or unless the data subject gives his or her consent for the data to be used otherwise.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The Data Protection Act (2018) makes no reference to the quality, currency or accuracy of personal data and relies on the provisions of the GDPR. The GDPR states that the personal data processed shall be accurate and where possible kept up to date. The data subject is also granted the right to request the rectification of inaccurate personal data; inaccuracy of data gives the data subject the right to restrict the data controller from further processing.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

While the Data Protection Act (2018) makes no mention of measures regarding minimisation or retention periods with regard to personal data, the GDPR requires the data controller to establish concrete retention periods for all personal data collected, which period shall be notified to the data subject prior to the collection of data. Should such a retention period not be easily determinable, the data controller shall inform the data subject of the criteria to be applied when determining such retention period. The principle of data minimisation requires the data controller to collect only personal data necessary for established processing purposes.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The GDPR provides that personal data is to be collected for a specified, explicit and legitimate purpose and that if such data is further processed, the processing has to be compatible with the initial purpose of collection. Additional processing may only be conducted following prior notification and provision of information to the data subject.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The Act (2018) acknowledges that in cases of data collected for historical, scientific, statistical and archiving purposes, the same data can be used for other purposes, in which case data controllers and processors must fully abide by the provisions of the Act (2018) and the GDPR.

The Restriction of the Data Protection (Obligations and Rights) Regulations provides that data collected in terms of the parameters of the same regulation can be processed only for the purpose of its

collection, unless the law provides otherwise or the data subject gives their consent for the data to be used otherwise.

Security

20 Security obligations

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

The GDPR states that personal data is to be processed in an appropriately secure manner. The controller is obliged to include a general description of the technical and organisational security measures taken in its processing activities record. It is also stipulated that both the data controller and the processor are to implement technical and organisational measures to ensure an appropriate measure of security through encryption, pseudonymisation and integrity of the network systems, the creation of data protection policies and codes of conduct, among other measures.

The Restriction of the Data Protection (Obligations and Rights) Regulations also provides that the data controller must implement appropriate technical and organisational measures.

21 Notification of data breach

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 Protection Act (2018) makes no specific reference to notifications to supervisory authorities or individuals with regard to data breaches, and relies on the provisions of the GDPR.

The GDPR provides that when there is a personal data breach, the supervisory authority is to be informed by the controller without undue delay and in any case within 72 hours of the discovery of the data breach. Such period may only be extended in justified cases. In cases where the processor becomes aware of such a breach, the processor must immediately inform the data controller.

In cases of high risk, the breach must also be communicated to the data subject, through direct communication using clear and plain language. The controller may not be obliged to inform the data subject if appropriate technical and organisational protection measures were implemented, subsequent measures to mitigate the breach are taken and if it would involve a disproportionate effort to notify data subjects individually.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The GDPR provides for specific situations where a data protection officer is to be appointed, mainly if:

- the processing is conducted by a public authority, excluding courts acting in their judicial capacity;
- the processing of data occurs on a large scale by controllers and processors whose core activity is data processing; and
- the data controller and processor process special categories of data and data in connection to criminal convictions and offences on a large scale.

The Data Protection Act (2018) stipulates that the minister responsible for data protection can prescribe regulations to designate the mandatory appointment of a data protection officer in cases other than those already provided for by the GDPR.

In terms of the main responsibilities of a data protection officer, the GDPR states that the officer is to inform and advise the controller or processor on their obligations pursuant to the GDPR and other data protection laws, monitor the policies of the controller or processor in relation to the GDPR, cooperate with supervisory authorities and act as a contact point with such an authority, and provide advice on impact assessments. The data protection officer shall also be the point of contact with regard to matters concerning data protection within and without the organisation.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The Data Protection Act (2018) does not provide for the further keeping of internal records or for the establishment of internal processes or documentation, other than what is provided for in the GDPR. The GDPR provides that controllers shall keep a record of processing activities; processors are also obliged to maintain records of processing activities carried out on behalf of controllers. Both parties shall also maintain documentation relating to the appropriate technical and organisational structures present within their remit in compliance with the GDPR, which shall be available for consultation at any time.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The GDPR requires the application of the principles of data protection by design, which involves the implementation of appropriate measures, controls and processes to ensure data protection principles are adhered to without the need for additional action. Such measures may include pseudonymisation and anonymisation, while adhering to the principles of confidentiality, integrity and availability of personal data. The GDPR also includes the implementation of appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

Furthermore, the data controller shall carry out impact assessments where a type of processing in particular using new technologies is likely to result in a high risk to the rights and freedoms of natural persons; this shall be particularly required in cases where data processing involves the systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, where special category data is processed on a large scale and in cases of large-scale, systematic monitoring of public areas.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

The GDPR and the Data Protection Act (2018) do not require the registration or enrolment of data controllers or data processors with the Office of the Information and Data Protection Commissioner. The Maltese supervisory authority does, however, require the registration and publication of details pertaining to officially appointed data protection officers.

26 Formalities

What are the formalities for registration?

Not applicable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

As noted in question 25, the Maltese supervisory authority requires the registration and publication of details pertaining to officially appointed data protection officers.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The data controller shall have the right to outsource processing activities to third parties. Such processing must, however, be conducted by appointed data processors guaranteeing compliance with the GDPR. Data processors must be appointed in the form of a binding agreement in writing setting out 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. The agreement shall include:

- provisions binding the processor to conduct processing activities solely upon the data controller's documented instructions;
- the imposition of confidentiality clauses upon individuals conducting processing activities;
- the implementation of measures aimed at assisting the data controller in complying with data subject requests;
- the implementation of appropriate technical and organisational measures to ensure the security of the personal data being processed;
- the duty to assist data controllers in collaborating and requesting approval from the supervisory authority where necessary; and
- provisions regarding the appointment of sub-processors, which shall only be appointed following the specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

The data processor shall be given clear written instructions with regard to the disposal or return of processed personal data upon termination of the parties' relationship, which methods of disposal or return shall be determined solely by the data controller. The data processor shall also be bound to provide the data controller with all the information necessary to prove compliance with the provisions of the GDPR.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

See questions 34 and 35.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The transfer of personal data outside Maltese jurisdiction is not prohibited by the legal regime currently in force and may be affected freely within European Union territory, as well as to third countries and international organisations. Transfers of personal data to third country jurisdictions and international organisations shall take place only in favour of processing entities able to comply with the conditions contained within the GDPR, allowing for adequate protection to data subjects as contained within Chapter V of the same regulation.

Where the European Commission has determined that a third country or an international organisation offers adequate levels of protection (an adequacy decision), such transfers may take place freely and without the need for specific authorisation; in the absence of such adequacy decisions, the transfer of personal data to a third country or an international organisation shall only be permitted provided that the controller or processor has appropriate safeguards in place and upon condition that enforceable data subject rights and effective legal remedies for data subjects are available in the said third country jurisdiction.

'Appropriate safeguards' include:

- a legally binding and enforceable instrument between public authorities or bodies;
- the application of binding corporate rules;
- the application of standard data protection clauses adopted by the European Commission;
- the application of standard data protection clauses adopted the Maltese supervisory authority and approved by the European Commission;
- the use of an approved code of conduct coupled 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
- the presence of an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including those necessary for the protection of the rights and freedoms of data subjects.

Without prejudice to the above, the GDPR specifically excludes the transfer of personal data to third country jurisdictions pursuant to court judgments or the decision of a third country administrative authority, unless such request is enforceable by virtue of an international agreement or treaty binding the European Union or Malta and the third country forwarding such request.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Cross-border transfers of personal data to third countries or international organisations shall require the Commissioner's authorisations in the absence of an adequacy decision or where the appropriate safeguards mentioned above are not in place; such requirement for appropriate safeguards may also be fulfilled through the use of contractual clauses between the parties to the data transfer, as well as through provisions inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights, subject to the Commissioner's authorisation. Such transfers shall only be permitted in cases where the proposed transfers are not repetitive, where they concern a limited number of data subjects and where they are required for the pursuit of a data controller's legitimate interest.

36 Further transfer

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

Onward transfers of personal data from a third country or an international organisation to another third country or another international organisation are subject to the same conditions imposed upon initial transfers to third countries or international organisations.

Update and trends

The coming into force of the GDPR has seen numerous businesses rushing to ensure that they become compliant with the newly introduced regulation. With distributed ledger technologies and most famously blockchain technology having gained global recognition, many are asking whether GDPR will affect these technological developments and, more importantly, the effect its adoption may have upon the various sectors applying blockchain technology as a preferred solution. Seeing as the GDPR grants the right of erasure to data subjects, one is yet to see how this will affect blockchain technology when it is being used in practice, seeing as the technology itself aims to be immutable and thus technically exempt from such data subject rights.

Rights of individuals

37 Access

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

Article 15(3) of the GDPR grants data subjects the right to request a copy of their personal data being processed by the data controller. Such access shall be provided free of charge and in an easily accessible electronic format should the data subject's request be made by electronic means. Additional copies of the said data may also be provided at a reasonable, elective fee covering administration costs incurred by the data controller.

While this access right is generally considered to be universal, it may be lawfully curtailed in particular instances whereby disclosure of personal data may result in the data controller's failure to meet its legal obligations under other laws currently in effect in Malta, such as the Prevention of Money Laundering Act.

38 Other rights

Do individuals have other substantive rights?

Under the GDPR's provisions, the data subject is also afforded the right to rectification of personal data, the right to erasure of personal data, the right to restrict processing, the right to data portability, the right to object to processing of personal data and the right to lodge a complaint before the relevant supervisory authority with regard to issues relating to the processing of personal data.

The GDPR also prohibits the processing of special categories of personal data, including 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, save for specific instances or upon the data subject's granting of explicit consent. Furthermore, data subjects have the right not be subjected to decisions based solely on automated decision-making processes, provided that such decisions produce legal effects or other significant effects that may affect the data subject's rights and freedoms.

39 Compensation

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 provisions of article 30 of the Data Protection Act (2018), data subjects are afforded the right to institute an action for damages against data controllers or data processors processing personal data in contravention of the provisions of the GDPR or of the same Act. The Maltese Civil Courts are empowered to determine the amount of damages representing loss of wages or other earnings, as well as moral damages due to the affected data subject. While claims for damages pursuant to loss of wages or earnings must be necessarily backed by evidence proving mathematically determinable financial losses, claims for moral damages, including injury to feelings, are uncapped and are determined by the civil courts. Such rights to legal remedy shall not preclude the affected data subject from lodging a formal complaint with the Maltese supervisory authority requesting the investigation of alleged breaches of data protection legislation.

40 Enforcement

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

Recourse to the right to compensation, representing monetary losses or moral damages, may be exercised personally by affected data subjects through the filing of a sworn application before the First Hall of the Civil Courts of Malta instituting an action for damages against the data controller or data processor processing personal data in contravention of applicable law. Such actions shall be instituted within a period of 12 months from the date when the data subject became aware, or ought to have reasonably become aware, of such a contravention, whichever is the earlier.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The law does not provide for any further exemptions or restrictions.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

The Data Protection Act (2018) establishes the Information and Data Protection Appeals Tribunal, allowing for appeals to be filed against legally binding decisions taken by the Commissioner within 20 days from the service of the Commissioner's decision. The Tribunal shall be composed of a chairperson and two additional members representing the interests of data subjects and of data controllers and data processors respectively. The Tribunal's decisions are furthermore subject to the right of appeal before Malta's Courts of Appeal.

gtg ADVOCATES

Ian Gauci **igauci@gtgadvocates.com**
Michele Tufigno **mtufigno@gtgadvocates.com**

66, Old Bakery Street
Valletta
VLT1454
Malta

Tel: +356 2124 2713
Fax: +356 2124 2714
www.gtgadvocates.com

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Subsidiary Legislation 586.01, titled the Processing of Data (Electronic Communications Sector) Regulations, implements the provisions of Directive 2002/52 EC of the European Parliament and Council. The Regulations address the consent required from users before sending unsolicited communication, including SMS and cookies, with the latter being stored on devices.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

The GDPR addresses direct marketing, but does not distinguish between electronic and non-electronic marketing. In cases of direct marketing, the data subject has the right to object to the processing of their data for marketing purposes.

Subsidiary Legislation 586.01, titled the Processing of Data (Electronic Communications Sector) Regulations implementing the provisions of Directive 2002/52 EC of the European Parliament and Council, also provides that a person cannot use electronic communication services to make unsolicited communication for the purpose of direct marketing by using automated calling machines, emails or facsimile machines. However, the Regulations stipulate that a person may use the contact details obtained from a customer in relation to the sale of a product or a service to directly market its own similar products or services.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

The GDPR and the Data Protection Act (2018) do not contain specific provisions regulating the offering of cloud services within the context of data protection and privacy laws; the general principles applied to data processors and data controllers are thus applicable to cloud service providers.

Mexico

Abraham Díaz Arceo and Gustavo A Alcocer
OLIVARES

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legal framework for PII protection is found in article 6 of the Mexican Constitution; and in the Federal Law for the Protection of Personal Information Held by Private Entities, published in July 2010, its Regulations, published in December 2011, the Privacy Notice Rules, published in January 2013, the Binding Self-Regulation Parameters, also 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 PII 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 PII and protects individual data subjects (individuals); it is a federal law of public order, which makes its provisions applicable and enforceable at a 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. This Law regulates the use and processing given to the PII by PII data controllers (PII controllers) and PII processors, thus providing several rights to individuals and obligations to PII controllers and PII processors, in order to ensure the privacy 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.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is the authority responsible for overseeing the Law. Its main purpose is the disclosure of governmental 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 PII controllers and PII 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.

3 Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with 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 PII instead of a sectorial model, in Mexico the INAI is the only data protection authority in charge of the protection of personal information.

Furthermore, 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, in order to help in the protection of personal information.' However, so far we have no knowledge of any matter in which the INAI has been expressly requested to cooperate with international authorities.

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 PII, 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 above law.

4 Breaches of data protection

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 (MGDW) for PII controllers and PII processors. Depending on the seriousness of the breach and specific behaviour and conduct (profit-making with PII or the methods used to get consent for the use of PII), it may lead to criminal penalties, which are sanctioned with three months to five years of imprisonment. This also depends on the nature of the PII (penalties are doubled if the personal data is considered by law as sensitive personal data).

In addition, related conduct may be sanctioned under the Criminal Code, such as professional secrecy breaches and illegal access to media systems and equipment.

Scope

5 Exempt sectors and institutions

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

The Law applies to non-public individuals and entities that handle PII. In addition, the following non-public persons and entities are excluded from the application of the Law:

- credit information bureaux or companies, where such companies are specially regulated by the Law for the Regulation of Credit Information Companies; and
- persons who handle and store PII exclusively for personal use and without any commercial or disclosure purposes.

Also, from January 2017, the 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.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Law covers PII 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 communication (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.

- Article 166-bis of the Federal Criminal Code sanctions with imprisonment from three months to up to three years 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 MGDW, 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, the person who reveals, divulges or improperly uses any information or images obtained from the intervention of a 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, with the aim of collecting a debt from them, or having them comply with an agreement.
- 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 provided by the consumer in a confidential manner, and consequently said information cannot be transmitted to other different suppliers, unless consented by the consumer or ordered by competent authorities.

7 Other laws

Identify 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, so far 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 PII there is a referral to the rules set forth 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).

8 PII formats

What forms of PII are covered by the law?

As previously noted, the Law covers PII regardless of the means or media used for its storage, process or organisation. Such means or formats include:

- digital environment (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 PII stored in the cloud);
- electronic support (storage that can be accessed only by the use of electronic equipment that processes its contents in order to examine, modify or store the PII, including microfilm); and
- physical support (storage medium that does not require any device to process its content in order to examine, modify or store the PII or any plain sight intelligible storage medium).

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Mexican PII protection laws are not limited to PII 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 being applicable 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 PII protection apply: to company 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 PII; and when the PII controller is not established in Mexican territory but the person designated as the party in charge of the control and management of its PII (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.

10 Covered uses of PII

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

All processing or use of PII is covered by the Mexican legal framework.

Mexican PII protection law makes a distinction between PII controllers and those who provide services to controllers, where the latter are independent third parties who may be engaged by the PII controller in order to be the parties responsible for the PII processing and handling. While it is not mandatory to have this third-party service provider, should a company (PII controller) engage such services, it shall have a written agreement stating all the third party's responsibilities and limitations in connection with the PII.

In virtue of this obligation of PII controllers to execute an agreement with any PII processor they use, the duties acquired by the PII processor must be the same as those imposed by the Law on the PII controller.

Legitimate processing of PII

11 Legitimate processing – grounds

Does the law require that the holding of PII 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 PII:

- legality: PII controllers must always handle PII in accordance with the law. All personal data shall be lawfully collected and processed, and its collection shall not be made through unlawful or deceitful means;
- consent: PII controllers must obtain consent from individuals for the processing and disclosure of their PII. In this regard, consent of individuals shall not be required if:
  - PII is contained in publicly available sources;
  - PII cannot be associated with the individual, or if by way its structure or content cannot by associated with the individual;
  - PII processing is intended to fulfil obligations under a legal relationship between the PII controllers and individuals;

  - there exists an emergency situation in which the individual or its properties may be potentially damaged;
  - PII 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 PII, without the required consent;
- information: PII controllers must notify the individual of the existence and main characteristics of the processing that will be given to the PII;
- quality: PII handled must be exact, complete, pertinent, correct and up to date for the purposes for which it has been collected;
- purpose (the 'finality principle'): PII may only be processed in order to fulfil the purpose or purposes stated in the privacy notice provided to the individual;
- loyalty: PII controllers must protect individuals' interests when handling their PII;
- proportionality: PII controllers may only handle the PII necessary for the purpose of the processing; and
- responsibility: PII controllers are responsible for the processing of the PII under their possession.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The law makes a distinction regarding 'sensitive' PII. This information is deemed the most personal of the individual, and if mistreated, could lead to discrimination or to general risk to the individual (i.e., racial or ethnic origin, present or future health status, genetic information, religion, political opinions, union membership or sexual orientation).

In view of this, the Law provides more stringent rules for the processing of this sensitive PII, such as the obligation for PII controllers to always get written and express consent from individuals for the processing of their sensitive PII. Likewise, PII controllers may not hold sensitive PII without justified cause pursuant to the purpose of the processing.

Several additional limitations apply to the general handling of this type of information (eg, PII controllers must use their best efforts to limit the processing term of sensitive PII, the privacy notice must expressly point out the nature of such information when required; and, as previously pointed out, when it comes to penalties for the breach or mistreatment of PII, these may double when processing sensitive PII).

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The PII 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 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 PII controller;
- PII that would be subject to processing;
- the purpose of the processing;
- the mechanisms provided by the PII 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 PII;
- any transfer of the PII to be made, if applicable;
- the procedure and vehicles in which the PII controller will notify individuals about modifications to the privacy notice;
- the procedure and means by which the PII controller should notify the individuals of any modification in such privacy notice; and
- regarding sensitive PII, the privacy notice shall 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.

14 Exemption from notification

When is notice not required?

A privacy notice is not necessary when:

- exemption is available in a specific provision of applicable law;
- the data is available in public sources;
- PII data is subject to a prior dissociation procedure (anonymised data);
- there is an existing legal relationship between the individual and the PII 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.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The Law provides individuals with 'ARCO' rights: to access (the right to know what information is being held and handled by the PII controller), rectify (the right to request at any time that the PII controller correct the PII that is incorrect or inaccurate), cancel (the right to request the PII controller to stop treating their PII) or oppose (the right to refuse) the processing of their PII.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

As discussed in question 11, PII has to fulfil the standard of quality (PII should be exact, complete, pertinent, correct and up to date).

Quality is presumed when PII is provided directly by the individual, and remains such until the individual does not express and prove otherwise, or if the PII controller has objective evidence to prove otherwise. When personal data has not been obtained directly from the individual, the PII controller must take reasonable means to ensure the quality standard is maintained.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The Law provides a 'need to hold basis'; PII controllers must not hold PII any longer than the time required to fulfil its purpose (as stated in the privacy notice). After the purpose or purposes have been achieved, a PII controller must delete the data in its collection after blocking them for subsequent suppression.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

As discussed in question 11, the Law does provide a 'finality principle', whereby a PII controller is restricted to using the PII only in order to fulfil the purpose or purposes stated in the privacy notice provided to the individual, the purpose of which must comply with the legality standard. If the PII 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 purposes.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The PII controller is not allowed to use PII 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.

Security

20 Security obligations

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

PII controllers or entities in charge of processing PII must take and observe various security measures for the protection of the PII, 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 PII.

In addition, certain physical measures such as actions and mechanisms – technological or otherwise – 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 to the information is by authorised personnel only;
- the aforementioned access is only in compliance with authorised personnel's required activities in accordance with 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 PII.

Other actions that must be taken include:

- making an inventory of the PII 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 PII of the company);
- establishing security measures applicable to PII;
- conducting an analysis for 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 PII; and
- maintaining a register of the PII databases.

21 Notification of data breach

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 accordance with the Law, PII 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 to the individual of the measures that the PII controller may take to protect his or her interests;
- any corrective actions taking place immediately; and
- any means by which the individual may find more information on the subject.

In the case of a violation of PII, the PII 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, so far Mexican law does not include an obligation for private PII controllers to notify the supervisory authority. In the case of government entities, they indeed have an obligation to notify the INAI of any data breach.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

It is mandatory for the PII controller (or manager) to appoint an officer (person or department) in charge of the PII, who will be in charge of attending to and taking care of individual requests in order to exercise any of their rights provided by the Law. Likewise, this officer must promote the protection of PII within the company.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Although the Law does not specify record keeping as a mandatory requirement, as previously mentioned, it is recommended that PII controllers have a PII database, as well as a register on the means and systems used for the storage of those databases, in order to provide the maximum security for the PII under their possession or control.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The law does not yet include an obligation to adopt new processing operations such as a privacy-by-design approach. However, PII controllers must carry out privacy impact assessments in order to determine the security measures to be adopted, as set forth in articles 60 and 61 of the Regulations of the Federal Law for the Protection of Personal Information Held by Private Entities.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There is no need for PII controllers or processors to register with the INAI; however, the INAI has the authority to request a surprise inspection to monitor that PII controllers are complying with the Law and Regulations.

26 Formalities

What are the formalities for registration?

Not applicable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

Update and trends

It is relevant to mention that on 12 June 2018, a decree by which Mexico formally accedes to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) and its Protocol was published in the Official Gazette. This will lead Mexico to bring its level of protection of PII in line with the international standards set forth by the European Council, and will provide tools for the effective and safe international exchange of PII.

29 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

No other public transparency duties are imposed on PII controllers.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

In order to explain the regulations on transfer of PII, it must first be understood that the Law defines the transfer of PII as the communication of PII to third parties, whether inside or outside Mexico, other than the PII controller (PII controlling company), in which the third party has to comply with the provisions set forth in the privacy notice of the PII controller.

The transfer of PII to entities that provide PII processing services is not construed as a transfer of PII per se; therefore, any such transfer of PII will be the responsibility of the PII controller and, thus, the PII controller will be liable for any risk or breach in the PII information, which is why it is mandatory to regulate business relationships with PII processors through the execution of agreements, by virtue of which PII processors acquire the same obligations and duties as PII controllers.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Any transfer of PII (as defined by the Law) must be made with the individual's consent, unless otherwise provided by Law (certain exceptions to consent apply). PII disclosure to other recipients must be made under the same conditions as it was received by the PII controller, so, in the case of such disclosure, the PII controller will be able to demonstrate that it was communicated under the conditions as the individual provided such PII. The original PII Controller always has that burden of proof in these cases.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The following transfers are allowed without restrictions:

- where the transfer is made pursuant to a law or treaty to which Mexico is 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 PII controller or to a parent company or any company of the same group as the PII 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 PII 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 PII controller and the individual.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

There is no mandatory notification or authorisation required from supervising authority. The Law only provides that the PII controller may, if it deems necessary, request an opinion from the INAI regarding the compliance of any international PII transfer with the Law.

36 Further transfer

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 not subject to restriction or authorisation.

Rights of individuals

37 Access

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

Among the main rights of individuals (ARCO rights – see question 38) is the right to access a copy of the information being held and treated by the PII 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.

38 Other rights

Do individuals have other substantive rights?

In addition to the right of access, as previously pointed out, the Law provides individuals with their ARCO rights: right to access, rectify, cancel (request the PII to stop treating their PII) or oppose (eg, refuse) the processing of their PII.

39 Compensation

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 INAI is entitled to declare neither damages nor compensations in favour of any individuals. Therefore the breach of any PII law does not automatically grant monetary damages or compensations to any PII owner.

It is important to mention that under Mexican legislation damages must be claimed and proven through a civil law action. In addition, injury to feelings can also be claimed as moral damage, but moral damages must also be claimed through a civil action before Mexican civil courts. This means that any PII owner has to prosecute first an administrative action before the INAI in order to prove the breach of the law, and after that, to initiate an independent civil law action, before civil courts, in order to collect any damages, or loses, or to claim any compensation derived from any moral damage.

40 Enforcement

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

The rights are exercisable by the INAI. The process is initiated either by a filing by an affected individual or directly by the INAI as a result of any anomalies found during a verification procedure.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Aside from the limitations and exclusions already described herein, the Law does not include any additional derogations, exclusions or limitations.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes. Since the INAI is an administrative authority, any of its resolutions can be challenged through a nullity trial before the Federal Court for Administrative Affairs, and later on through a Constitutional rights action known as Amparo suit.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The Law specifically refers to the use of PII in the cloud; the Law provides a list of requirements with which the third party providing these types of storage service must comply in order to ensure the safety of the PII to be uploaded therein.

Furthermore, when PII controllers use remote or local means of electronic communication, optical or other technology mechanisms, that allow them to collect PII automatically and simultaneously at the same time that individuals have contact with PII (cookies or web beacons), the individuals must be informed, through a communication or warning duly placed in a conspicuous location, with regard to the use of these technologies and the fact that PII has been collected, as well as the process to disable such access, except when the technology is required for technical purposes.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

The Law does not provide any specific rules on marketing by email, fax or telephone; nonetheless, any such contact with individuals is treated as PII and any marketing through those media will, therefore, be regulated in accordance with the Law.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Mexican law regulates the processing of PII 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 in a flexible manner, 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 with respect to 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 authority 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 PII.

No guidelines have yet been issued to regulate the processing of PII in cloud computing.

OLIVARES

Abraham Díaz Arceo **abraham.diaz@olivares.mx**
Gustavo A Alcocer **gustavo.alcocer@olivares.mx**

Pedro Luis Ogazón 17
Col. San Ángel
01000 Mexico City
Mexico

Tel: +52 55 53 22 30 00
Fax: +52 55 53 22 30 01
www.olivares.com.mx

Portugal

Helena Tapp Barroso, João Alfredo Afonso and Tiago Félix da Costa

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legislative framework for the protection of PII applicable in Portugal is currently (as from 25 May 2018) that resulting from the direct application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation, or GDPR). Currently (July 2018) there is no specific national legislation providing for specific rules in the context of the GPDR, although a proposal is under discussion in parliament and may be expected within the next few months. The previous dedicated Portuguese data protection law governing personal data processing that was issued in 1998 (Law No. 67/98 of 26 October 1998 (the DPA)) has not, as such, been revoked, although a number of its provisions must be deemed to be derogated by provisions of the GPDR. 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. This initial law was based on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), adopted by the Council of Europe.

Portugal has relevant national constitutional privacy provisions, as article 35 of the Portuguese Constitution (on the use of computerised data) sets forth the main relevant principles and guarantees that rule PII protection.

International instruments relevant for PII protection have also been adopted in Portugal, as is the case of the following:

- the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108);
- the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), of which article 8 is specifically relevant for PII protection; and
- the Charter of Fundamental Rights of the European Union (ie, articles 7 and 8).

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The National Commission for the Protection of Data (CNPD) is the authority responsible for overseeing the DPA in Portugal.

The CNPD (its members or delegated staff) have powers to require information on PII processing activities from public or private bodies and hold rights of access to the computer systems supporting PII processing, as well as to all documentation relating to the processing and transmission of PII, 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 PII;
- exercise investigative powers related to any PII processing activity, including PII transmission;
- exercise powers of authority, particularly those ordering the blocking, erasure or destruction of PII or imposing a temporary or permanent mandatory order to ban unlawful PII processing;
- issue public warnings or admonition towards PII owners failing to comply with PII 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.

This is a subject matter that will also be amended by the local law project under discussion, to be adapted in line with the provisions of the GDPR, namely in accordance with articles 51, 57 and 58.

3 Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with 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 of the GDPR on cooperation and consistency, pursuant to article 51(2), 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.'

4 Breaches of data protection

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. Currently there is no specific national legislation providing for specific rules in the context of the GPDR, although a proposal is under discussion in parliament and may be expected within the next few months. The proposal includes provisions on ranges of fines (minimum and maximum) and classifies infringements according to their nature and gravity, in line with artcle 83 of the GDPR.

Sector-specific legislation for the protection of PII in the electronic communication business activity (applicable, for example, to PII owners that are telecom operators and internet service providers) foresees much higher administrative fines for data protection law breaches (which may go up to a maximum of €5 million).

Criminal offences are punished with imprisonment of up to two years or a 240 day-fine (the relevant day-fine amount being fixed by the judge within a range between €5 and €500, depending on the financial situation and personal and family expense level of the offender), both of which can be aggravated to double the amount.

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 PII blockage, erasure or total or partial PII destruction, among others.

Criminal offences are subject to prosecution by the Public Prosecutor and their application must be decided by the criminal courts.

Scope

5 Exempt sectors and institutions

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 covered by the GDPR are in its scope, therefore covering PII processing by both public and private entities.

An application exemption was previously foreseen by the DPA for PII processing carried out by natural persons in the course of purely personal or domestic activities, and this is kept under article of 2(2)(c) of the GDPR.

The provisions of the DPA apply to the processing of personal data regarding public security, national defence and state security, without prejudice, however, to special rules contained in international law instruments to which Portugal is bound, as well as specific domestic laws on the relevant areas.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

A number of issues are covered by specific laws and regulations.

Video surveillance and surveillance cameras for defined purposes are the object of specific laws, as is the case, among others, of:

- Law No. 1/2005 of 10 January 2005 (subsequently amended and republished by Law No. 9/2012 of 23 February 2012) on the installation in public areas and use of surveillance through video cameras, by national security forces (for the protection of public buildings, including premises with interest for defence and security, 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 (and Regulation No. 273/2013 of 20 August 2013).

7 Other laws

Identify 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 PII 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 41/2004 of 18 August 2004, which implemented Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, or ePrivacy Directive) as amended by Law 46/2012 of 29 August 2012, implementing Directive 2009/136/EC (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 above referred Directive 2002/58/EC. The reform of ePrivacy legislation currently taking place in the EU 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 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC have also been implemented in Portugal through Law No. 32/2008 of 17 June 2008 on the retention and transfer of such PII for the purposes of the investigation, detection and prosecution of serious crime by competent authorities.

Other 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 a number of 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.

The retention of PII by electronic service providers is regulated by Law No. 32/2008 of 17 June 2008.

Law No. 41/2004 of 18 August 2004 as amended by Law 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.

8 PII formats

What forms of PII are covered by the law?

The legislation applicable in Portugal covers PII processed by totally or partially automatic means as well as PII that forms part of a (manual) filing system or is intended to form part of such systems (GDPR). This was also the case under the DPA.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The Portuguese DPA covers PII processing carried out in the context of the activities of an establishment of the PII owner located in Portuguese territory or in a place where Portuguese law applies by virtue of international public law.

The DPA also applies to processing carried out by a PII owner established outside the European Union area but who makes use of automated or non-automated means for processing located in Portuguese territory, with the exception of means or equipment located in Portugal to serve the purposes of mere transit of PII through the country.

The DPA covers video surveillance and other forms of PII collection, processing and broadcast consisting of sound or image, whenever the owner is located in Portugal or uses a network access provider established in Portuguese territory.

The GDPR territorial scope, as defined in article 3, nevetheless fully applies.

10 Covered uses of PII

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

Although the DPA includes a number of provisions that refer to processors or processing services, the main direct legal obligations contained in the DPA are applicable to PII owners.

Although administrative penalties and criminal infractions refer primarily to PII owners (while applicable to the breach of specific PII owner legal duties) penalties are not exclusively applicable to the same entities (eg, unauthorised access to PII, tampering or destruction of PII and others is not restricted to a PII owner action).

All processors' duties directly resulting from the GDPR (and, naturally, all controllers' duties) apply directly in Portugal.

Legitimate processing of PII

11 Legitimate processing – grounds

Does the law require that the holding of PII 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 the GDPR, particularly those in articles 6 and 9 on the requirement that the holding of PII be legitimised on specific grounds, fully apply.

In line with article 6 of the GPDR, PII 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;
- processing of the PII is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the latter prior to entering into a contract;
- PII processing is necessary for compliance with a legal obligation to which the PII owner (controller) is subject;
- PII processing is necessary in order to protect the vital interests of the individual or of another natural person;
- PII 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
- PII processing is necessary for the purposes of 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.

The Portuguese DPA also required that the holding of PII was legitimised on specific grounds.

In the case of non-sensitive data, processing, under the DPA, was legitimate on the following grounds:

- consent from the individual;
- performance of a contract or contracts to which the individual is a party;
- completion of pre-contractual steps, at the request of the individual, prior to entering into a contract or declaring his or her will to negotiate;
- compliance with legal obligations impending over the PII owner;
- protection of vital interests belonging to the individual in cases where the latter is physically or legally incapable of providing consent;
- performance of a task carried out in the public interest or in the exercise of official authority vested in the PII owner or in a third party entity to whom the PII is disclosed; and
- need resulting from the legitimate interests of the PII owner (or third parties to whom the PII is disclosed), unless overridden by the individual's fundamental rights, freedoms or guarantees.

These must be read in light of the GDPR.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

More stringent rules apply in the case of the 'special categories of data' indicated in article 9 of the GDPR. This refers to the processing of genetic PII, biometric PII, PII concerning health, data concerning the individual's sex life or sexual orientation, PII revealing 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 PII is prohibited with the exceptions provided for in article 9 of the GPDR. Currently the DPA does not provide for any additional exceptions.

In the case of PII relating to health or sex life, including genetic data, processing is also legitimate on medical grounds (preventative 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 PII owner, provided the latter are not overridden by the individual's fundamental rights and freedoms.

Processing of personal data 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 PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The DPA required owners of PII to notify individuals whose data they hold of the following information, at the time of collection of the PII, (except where the individuals already hold such information):

- the PII owner's identity and, where applicable, that of the owner's representative;
- the purposes of the PII processing; and
- other relevant information, including, at least, the following:
  - the PII recipients or category of recipients;
  - the statutory or voluntary nature of responses on PII required from the individual (and the consequences of not providing a response);
  - information that PII may circulate on the network without security measures and may be at risk of being seen or used by unauthorised third parties, when the PII is collected on an open network; and
  - the existence and conditions for the exercise of the individual's rights of access to PII and correction thereof.

Where the PII is not obtained by the PII owner directly from the individual, notification should take place at the time the first processing operation takes place or, if disclosure to third parties is envisaged, at the time disclosure first takes place.

Information requirements provided for in articles 13 and 14 of the GDPR are now applicable and supersede, as may be applicable, those that were contained in the DPA.

14 Exemption from notification

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) and where personal data has not been obtained from the data subject;
- 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 PII 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.

The DPA provides that notice is not required if processing is carried out solely for journalistic purposes or for literary or artistic expression purposes.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

PII owners must offer individuals whose PII they hold the rights of access, 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 as provided for in the GDPR.

The right of access comprises the individual's entitlement to obtain from the owner confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to the personal data and to all the information provided for in article 15(1)(a) to (h) and (2) of the GDPR.

The right of access also entitles the individual to obtain from the owner a copy of the PII undergoing processing.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

PII processed must be relevant, accurate and, where necessary, kept up to date in relation to the purpose for which it is held.

The PII owner is required to take adequate measures to ensure that PII that is inaccurate or incomplete, in light of the processing purpose, is erased or corrected.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The amount of PII that may be held is limited to that which is strictly adequate, relevant and not excessive in relation to the purpose for which it is collected and further processed.

The DPA does not specify allowed retention periods, the general rule being that the PII 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 CNPD that indicate, for specific purposes, the length of time the authority considers certain categories of PII may be held, which may still be taken into account in the context of the GDPR.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

As a rule, the finality principle was already applicable under the DPA. This is reinforced under the GPDR under the principles relating to the processing of personal data provided for in article 5 of the GDPR. PII may only be collected for specific, express and legitimate purposes and may not be subsequently used for purposes that are incompatible with the same.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Prior to the GDPR, the DPA provided that the CNPD may authorise, on an exceptional basis, the use of PII for purposes that differ from those that determined its collection, subject to the legally applicable PII quality and processing lawfulness principles. Currently, this is ruled by the GDPR, particularly by the provisions of article 6(4).

Security

20 Security obligations

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

Under article 32 of the GDPR, the owner and the service provider are subject to implementing appropriate technical and organisational measures (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 risk of varying likelihood and severity for the rights and freedoms of individuals) to ensure a level of security for PII appropriate to the risk. The adequateness of the measures must be assessed taking into account security and in particular of the risks that are presented by the PII processing, particularly from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to PII 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 PII;
- 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 PII in a timely manner 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 DPA focuses the requirement to put in place appropriate technical and organisational measures on the PII owners appropriate to protect PII against:

- accidental or unlawful destruction;
- accidental loss or alteration;
- unauthorised disclosure or access (particularly where processing of the PII involves its transmission over a network); and
- any other unlawful forms of processing.

The DPA provides that when sensitive PII is processed the owner must implement measures that are appropriate to:

- control entry to the premises where such sensitive PII is processed;
- prevent the PII from being read, copied, altered, removed, used or transferred by unauthorised persons;
- guarantee that no unauthorised PII input or PII input knowledge, alteration or elimination occurs;
- keep the access of authorised persons to sensitive PII to the limits of authorised processing;
- guarantee recipient entity verification when the same PII processing includes transmission; and
- guarantee that logs or other types of registration are kept to allow sensitive PII input control.

The DPA requires that systems guarantee logical separation between PII relating to health and sex life, including genetic information and other PII.

21 Notification of data breach

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 DPA did not include a general obligation to notify the supervisory authority or individuals of data breaches. Previously, there was a sector-specific requirement to do so in the electronic communications sector. In this case, data breaches should be notified by the PII owner to the CNPD, without undue delay and, if the data breach was likely to adversely affect individuals (ie, telecom service subscribers or users), PII owners were already also subject to notifying the individuals, also without undue delay. In this case, the data breach is deemed to affect PII individuals negatively in cases where the data breach may cause identity fraud or theft or connected physical or reputational damage or humiliation.

Under the GDPR, the data breach notification obligations to the supervisory authority and communication of a personal data breach to the data subject provided for under articles 33 and 34 respectively, fully apply as from 25 May 2018. The CNPD has provided PII owners with specific online forms for data breach notification.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

In Portugal and under the DPA, the appointment of a data protection officer was not required. As from 25 May 2018, however, under the GDPR, it is mandatory for certain PII owners (controllers) and processors to appoint a data protection officer. This will be 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.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The previous DPA did not provide for any specific or general requirements for PII owners or processors to maintain internal records or establish internal processes or documentation. In fact, the previous rules were based on a prior recording of PII processing activities with the supervisory authority (CNPD). As from 25 May 2018, however, under article 30 of the GDPR, PII owners shall maintain a record of processing activities under their responsibility, except in the case of PII owners 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 PII (sensitive data referred to in article 9(1)) or PII relating to criminal convictions and offences. The same requirement applies to PII processors.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Under article 25(1) of the GDPR, the PII owner shall, both at the time of the determination of the means for processing the PII 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, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of individuals. This must be done taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing.

The requirements to carry out a prior assessment of the impact of the envisaged processing operations on the protection of PII under article 35 of the GDPR fully apply in Portugal as from 25 May 2018.

The law project currently under discussion includes a provision whereby this assessment would not be required in the case of PII processing that had been previously authorised by the CNPD.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

The PII owner is no longer required to notify the CNPD or obtain prior processing authorisation from the same entity before any PII processing activities are initiated (with the exception of the prior consultation with the supervisory authority before processing that is required from the PII owner under the terms of article 36 of the 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).

26 Formalities

What are the formalities for registration?

Not applicable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

The CNPD register (mainly authorisation decisions) that refers to registrations and authorisations issued prior to 25 May 2018 is open to public consultation, free of charge, on the authority's website (www.cnpd.pt/bin/registo/registo.htm), although the information available is not complete.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

There are no transparency duties additional to the GDPR requirements.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the previous Portuguese DPA, entities providing outsourced processing services qualify as 'processors'. The processor must only act on instructions from the PII owner, unless he or she is required to act by law.

The PII 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 PII owner.

The PII 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.

As from 25 May 2018, all requirements contained in article 28 of the GDPR apply.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosure of PII is generally subject to all the processing principles, restrictions and notification requirements contained in the GDPR and in the 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 PII 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 PII can be disclosed only to health professionals or other professionals also subject to the same secrecy duties.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The transfer of PII to another European Union member state or European Economic Area (EEA) member country is not restricted.

Transfer of PII outside these territories is restricted. In this case, transfer is permitted only when it is compliant with the DPA requirements and when the state to which PII is transferred ensures an adequate level of protection assessed in the light of all the circumstances surrounding PII transfer, with special consideration being given to the nature of PII 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.

PII 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 such country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. Transfer may also be made under contracts that follow the standard form model clauses approved by the European Commission.

Prior to the GDPR, the Portuguese authority did not accept binding corporate rules for the transfer of PII. This is now admitted under the terms of article 47 of the GDPR.

In addition, transfer to the US may be done under the EU–US Privacy Shield framework following the adoption on 12 July 2016 of the European Commission decision on the EU–US Privacy Shield.

In the absence of an adequacy decision pursuant to article 45(3) of the GDPR or of appropriate safeguards pursuant to 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):

(a) 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;
(b) 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;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the PII owner and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the individual or of other persons, where the individual is physically or legally incapable of giving consent; or
(g) the transfer is made from a register which according to EU or Portuguese law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Portuguese law for consultation are fulfilled in the particular case.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No prior notification requirements apply.

36 Further transfer

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 EU and EEA between PII owners apply equally in the case of transfers of PII to service providers (processors).

Rights of individuals

37 Access

Do individuals have the right to access their personal information held by PII 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 PII owners. The DPA does not contain specific provisions on formalities for the exercise of this right of access, but it does establish that the access entitlement is not to be subject to restrictions, excessive delay or expense. The GDPR provides for the right of access, fully applicable in Portugal. (See question 15 for an indication of the entitlements comprising the individuals' right of access.)

When notifying the individuals whose PII they hold, the owners of PII must include information on the existence and conditions for the exercise of the individual's rights of access to PII and correction thereof (see question 13).

38 Other rights

Do individuals have other substantive rights?

Individuals are entitled to require the rectification of inaccurate information from the PII owner as well as the update of 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 information is meant for the purposes of 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 PII 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: the erasure of PII or restriction of processing concerning the individual, the right to object to processing and the right to PII portability.

39 Compensation

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 PII owner in breach of the PII 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.

40 Enforcement

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

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Not currently.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

PII owners can appeal against orders issued by the CNPD to the courts. In the case of decisions issued by the authority applying penalties for administrative misdemeanours, PII owners may appeal to the criminal courts. To appeal against decisions on authorisation or registration proceedings, competence lies with the administrative courts.

Specific data processing

43 Internet use

Describe 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 (ePrivacy Directive). The implementation came into effect on 30 August 2012.

The use of cookies requires the individuals' consent, after having been provided with clear and comprehensive information on the use of cookies, as well as on the categories of PII 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 tends to be seen as an opt-in solution.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of 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 by means of electronic mail also apply to SMS, EMS, MMS and other kinds of similar applications.

These rules do not exclude the possibility of a PII 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 PII 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 PII and on the occasion of each marketing message sent to the customer.

All direct marketing messages must identify the PII 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.

45 Cloud services

Describe 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 PII transfers and on the use of processors by PII owners will fully apply in the case of cloud computing services contracted by the owner.

MORAIS LEITÃO
GALVÃO TELES
SOARES DA SILVA

Helena Tapp Barroso **htb@mlgts.pt**
João Alfredo Afonso **joaoafonso@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 94
www.mlgts.pt

Russia

Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian Zimbler

Morgan, Lewis & Bockius LLP

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (the PD Law) is the main law governing personally identifiable information (personal data) in Russia. The PD Law was adopted in 2005 following the ratification of the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data. In general, the PD Law takes an approach similar to the EU Data Protection Directive and is based on the international instruments on privacy and data protection in certain aspects, but the Russian regulation places special emphasis on the technical (IT) measures for data protection. Notably, the PD Law has concepts similar to the one contained in the General Data Protection Regulation, which became effective in the EU on 25 May 2018. Data protection provisions can also be found in other laws, including Federal Law No. 149-FZ on Information, Information Technologies and Information Protection (2006) and Chapter 14 of the Labour Code of the Russian Federation (2001).

Further, numerous legal and technical requirements are set out in regulations issued by the Russian government and Russian governmental authorities in the data protection sphere, namely, the Federal Service for Communications, Information Technology and Mass Communications Supervision (known as Roskomnadzor), the Federal Service for Technical and Export Control (FSTEK) and the Federal Security Service (FSS). The regulations in this area are constantly being amended and developed.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The federal authority in charge of the protection of individuals' data rights (known under Russian law as 'personal data subjects') is Roskomnadzor. Roskomnadzor undertakes inspections of data processing activities conducted by companies that collect personal data (known under Russian law as 'data operators') and has the power to impose mandatory orders to address violations of data protection rules. Roskomnadzor's inspections can be either scheduled or extraordinary (e.g., upon receipt of a complaint from an individual). During the inspections (both documentary inspections and field checks), Roskomnadzor may review and request a data operator's documents describing data processing activities and inspect information systems used for data processing.

Administrative cases relating to violations of data privacy are initiated by Roskomnadzor and further considered by the court, which then makes an administrative ruling, for example, imposing administrative penalties.

Roskomnadzor is an influential body that interprets the provisions of the PD Law and addresses the problem areas in data protection practice. It publishes its views on various procedures for data protection (including on violations revealed during inspections) at its 'Personal Data Portal' at www.pd.rkn.gov.ru. Roskomnadzor also maintains two main state registers in the data privacy sphere – a register of data operators and a register of 'data operators in breach'. Another important authority is FSTEK. FSTEK is responsible for the development of technical regulations on data processing, including requirements for IT systems used in processing and measures required for the legitimate transfer of data. FSTEK is in some cases involved in the inspections carried out by Roskomnadzor. The authority issues working papers, opinions and interpretations of the PD Law related to the technical protection of personal data on its website at www.fstec.ru.

3 Legal obligations of data protection authority

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

Under article 23 of the PD Law, Roskomnadzor is entitled to cooperate with foreign data protection authorities, including on the international exchange of information on the protection of data subjects' rights. As part of this cooperation, Roskomnadzor organises conferences and public meetings and invites representatives of data protection authorities and professionals from other jurisdictions to participate.

4 Breaches of data protection

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

Under article 24 of the Russian Constitution, it is forbidden to collect, store, use and disseminate information on the private life of any person without his or her consent. This constitutional right is also protected under the PD Law. Under article 24 of the PD Law, persons violating the PD Law are subject to civil, administrative or criminal liability.

Under article 13.11 of the Code for Administrative Offences of the Russian Federation (the Administrative Code), a data operator (and, as the case may be, its officers and other relevant employees) may be liable for several breaches of personal data processing, including for:

- data processing without the individual's written consent when obtaining such consent is required;
- failure to publish the policy on data processing on the website; and
- failure to provide the individual with the information related to the processing of his or her data, with fines for an offence up to 75,000 roubles.

In addition, the Administrative Code imposes separate liability for failure to file or late filing to a government agency of necessary information on data processing activities (article 19.7 of the Administrative Code), with a fine of up to 5,000 roubles.

The Criminal Code of the Russian Federation provides criminal liability for unlawful collection or dissemination of personal data amounting to a personal or family secret without that person's consent, as well as the public dissemination of such data. Such criminal offences are punishable by monetary fines of up to 200,000 roubles, 'correctional labour' or even imprisonment for a period for up to two years with

disqualification for up to three years. Illegitimate access to computer information that has caused the destruction, blocking, modification or copying of personal data may also be subject to criminal liability, ranging from fines of up to 500,000 roubles and up to seven years' imprisonment. Under article 173.2 of the Criminal Code, the use of false documents accompanied with the illegal use of personal data is subject to criminal liability ranging from fines up to 500,000 roubles and up to three years' imprisonment.

In Russia, criminal penalties are imposed only on individuals and not on legal entities. The claim is usually filed by the prosecutor's office either after the office's own investigation or upon the request of Roskomnadzor or the injured individual. Civil liability in the data privacy sphere is provided by the Russian Civil Code (see question 39).

Scope

5 Exempt sectors and institutions

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

Article 1 of the PD Law expressly excludes from the scope of the PD Law any data processing in connection with record-keeping and the use of personal data contained in the Archive Fund of the Russian Federation, state secrets, as well as any processing related to the activities of the Russian courts. Further, the PD Law does not regulate data processing that is performed by individuals exclusively for personal and family needs, unless such actions violate the rights of other individuals.

In all other cases, the regulations of the PD Law are equally applicable to all organisations that collect personal data in Russia, irrespective of their sector or area of business. In certain industries it is common practice to develop standards for the processing and protection of personal data. Such 'industry standards' already exist for non-governmental pension funds, telecom operators, banks and healthcare organisations.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Article 23 of the Russian Constitution guarantees the right to privacy of personal life, personal and family secrets and correspondence for every individual. Therefore, as a general rule, the interception of communications or the monitoring and surveillance of an individual is allowed only with his or her explicit consent, unless such actions are performed in the course of investigative activities by state authorities. Certain limited activities related to the collection of personal data may be performed by private detectives with a state licence, as required by the Law of the Russian Federation No. 2487-1 on Private Detective and Safeguarding Activity (1992).

The PD Law sets out general principles for the use of personal data in the promotion of goods, work and services directly to potential consumers (via telephone, email or fax), including an obligatory opt-in confirmation. Electronic marketing procedures are also regulated by Federal Law No. 38-FZ on Advertising (2006) and the Law of the Russian Federation No. 2300-1 on Consumers' Rights Protection (1992) (see question 5).

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Specific provisions for the protection of certain types of personal data are covered by a variety of laws, which are nonetheless based on the general principles set out in the PD Law. For example, the protection of patients' data is regulated by Federal Law No. 323 on the Fundamentals of Protection of the Health of Citizens in the Russian Federation (2011). Personal data processing by banks and bank secrets are regulated by Federal Law No. 395-1 on Banks and Banking (1990). The principles of data handling by notaries and advocates are set out in the Fundamentals of Legislation of the Russian Federation on the Notariat (1993) and Federal Law No. 63-FZ on Advocacy and Advocate Activity in the Russian Federation (2002), respectively. In addition, the Labour Code of the Russian Federation, the Family Code of the Russian Federation, the Tax Code of the Russian Federation, Federal Law No. 98-FZ on Commercial Secrets and other laws regulate the processing of different types of personal data.

8 PII formats

What forms of PII are covered by the law?

The PD Law does not distinguish between personal data in paper or electronic format and is equally applicable to both. There are, however, separate rules applicable to processing data in paper and electronic format.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The PD Law does not specify its jurisdictional scope and generally applies to any legal entity, including any foreign entity with a legal presence in Russia, that collects personal data in Russia.

In addition, the PD Law provides for the local storage requirement, which applies to any data operator that processes the personal data of Russian citizens, regardless of its jurisdiction. Pursuant to the local storage requirement, an operator (for example, a company engaged in online business activity) is required to ensure that the recording, systemisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data is conducted only through the databases that are physically located in Russia. There are certain exceptions to this requirement. For example, data processing for the purposes of achieving the objectives of international treaties, for the purposes of implementation of an operator's statutory powers and duties, for professional activities of journalists or the lawful activities of mass media, or scientific, literary or other creative activities may be performed directly in the foreign databases.

10 Covered uses of PII

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

The PD Law does not use the terms 'data owners', 'data controllers' and 'data processors'. Instead, the PD Law distinguishes between 'data operators' and 'third parties acting on an instruction of a data operator'. A company engaged in data processing is a data operator, if it organises or carries out (alone or with other operators) the processing of personal data and, more importantly, determines the purpose, content and method of personal data processing.

Under article 6 of the PD Law, a data operator may assign or delegate data processing to a third party. Such a third party will be acting on an 'instruction of the operator' (see question 32). A third party does not need to obtain the separate consent of an individual to process his or her data within the same scope as permitted by the operator's instruction. It is the data operator who must ensure that all necessary consents are obtained. Arguably, all other requirements on data processing under the PD Law are equally applicable to both data operators and third parties acting on their instructions.

Legitimate processing of PII

11 Legitimate processing – grounds

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

The PD Law provides that any operation performed on personal data, whether or not by automatic means, such as collection, recording, organisation, storage, alteration, retrieval, consultation, use, transfer (dissemination or providing access), blocking, erasure or destruction, amounts to 'processing' of personal data and is subject to regulation. Thus, almost any activity relating to personal data constitutes 'processing' under the PD Law.

Any processing of personal data must be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purpose for which the data is processed must be explicit, legitimate and

determined at the point of data collection (article 5 of the PD Law). The data should be adequate, relevant and limited to a minimum necessary for the purpose of data collection and processing. This requires the data operator to assess regularly whether the processed data is excessive and the period necessary for processing such data.

As a general rule, the processing of personal data requires the consent of the individual. However, article 6 of the PD Law provides 10 general exemptions from the consent requirement, including instances where data is processed:

- under an international treaty or pursuant to Russian law;
- for judicial purposes;
- for the purpose of rendering state and municipal services;
- for performance of an agreement to which the individual is a party or under which the individual is a beneficiary or guarantor, including where the operator exercises its right to assign a claim or right under such an agreement;
- for statistical or other scientific purposes, on the condition that the data is anonymised;
- for the protection of the life, health or other legitimate interests of the individual, in cases where obtaining his or her consent is impossible;
- for the protection of the data operator's or third parties' rights or for the attainment of public purposes, provided there is no breach of an individual's rights and freedoms;
- for the purpose of mandatory disclosure or publication of personal data in cases directly prescribed by law;
- in the context of professional journalistic, scientific, literary or other creative activities, provided there is no breach of an individual's rights and freedoms; or
- if such data has been made publicly available by the individual or under his or her instruction.

Other exemptions from the consent requirement set out in articles 10, 11 and 12 of the PD Law may also apply depending on the type of data being processed.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Under the PD Law, all personal data is divided into the following categories:

(i) general data, which includes an individual's full name, passport details, profession and education, and in essence amounts to any personal data other than sensitive or biometric data;
(ii) sensitive data, which includes data relating to an individual's health, religious and philosophical beliefs, political opinions, intimate life, race, nationality and criminal records; and
(iii) biometric personal data, which includes data such as fingerprints, iris images and, arguably, certain types of photographic images.

The processing of data in categories (ii) and (iii) above must be justified by reference to a specific purpose and, in most cases, requires explicit written consent by an individual. Further, the processing of data relating to criminal records may only be carried out in instances specifically permitted by the PD Law and other laws.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

A data operator must notify an individual prior to processing his or her data, if such data was received from a third party. In particular, the data operator must give the individual notice of the following:

- the data operator's name and address;
- the purpose of processing and the operator's legal authority;
- the prospective users of the personal data;
- the scope of the individual's rights, as provided by the PD Law; and
- the source of data.

14 Exemption from notification

When is notice not required?

Notification of the data subject is not required if the data operator received the personal data directly from the concerned individual. Further, the requirement on the data operator to give notice before processing data received from a third party does not apply if:

- the individual has already been notified of the processing by the relevant operator;
- the personal data was received by the operator in connection with a federal law or a contract to which the individual is either a beneficiary or guarantor;
- the personal data was made publicly available by the individual or was received from a publicly available source;
- the personal data is processed by the operator for statistical or other research purposes, or for the purpose of pursuing professional journalistic, scientific, literary or other creative activities, provided there is no breach of the individual's rights and freedoms; and
- providing such notification would violate the rights or legitimate interests of other individuals.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

As a general rule, the individual will confirm the purposes and methods for the use of his or her personal data in the consent on processing granted to the data operator.

The individual has the right to control the use of his or her information upon obtaining access to the data by a request to the data operator (see question 37). In cases where the data processed by the operator is illegitimately processed, or is inaccurate or irrelevant for the purpose of processing, the individual may request that the data operator rectify, block or entirely delete his or her personal data or, alternatively, raise an objection against the purpose or method of processing with Roskomnadzor or in court.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

One of the basic principles of data processing is that the personal data kept by the data operator must be relevant, accurate and up to date. Therefore, the data operator must regularly review the data and update, correct, block or delete it as appropriate (articles 21 and 22 of the PD Law).

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

As a general rule, the personal data must be stored by the data operator for the period required to accomplish the purpose of processing. Such a period must be limited to a strict minimum. The period during which the personal data can be retained will usually depend on the retention rules for the documents containing the personal data.

For example, there are rules that cover the length of time certain personnel-related and other relevant records should be kept. Federal Law No. 125-FZ on Archiving in the Russian Federation (2004) and Order No. 558 of the Ministry of Culture of the Russian Federation on Approval of a List of Model Management Archival Documents Created in the Course of Activities of the Government Authorities, Local Self-Government Authorities and Organisations with Retention Period Specified (2012) set out minimum and maximum periods during which a company's documents, including documents containing personal data, should be retained. Depending on the nature of the document, such periods may vary from one year up to 75 years.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Under article 5 of the PD Law, any data processing must be carried out for specific, explicit and legitimate purposes, and the data collected or processed must be adequate, relevant and proportionate to the purposes of collection or further processing. The data operator must take all reasonable steps to ensure that inaccurate personal data is rectified or deleted. Article 5 of the PD Law obliges the data operator to destroy or depersonalise the concerned personal data, when the purposes of processing are met.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The PD Law does not provide for any exceptions from the finality principle.

Security

20 Security obligations

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

A number of complex security requirements apply to data operators and third-party service providers that process personal data under the operators' instructions. The PD Law only refers to general principles of data security and does not contain any specific requirements. The Regulation of the Russian Government No. 1119 dated 1 November 2012 describes the organisational and technical measures and requirements that must be taken to prevent any unauthorised access to the personal data. Following the adoption of the above regulation, FSTEK has issued a number of further regulations relating to technical measures aimed at the protection of processed data.

The data operator must take appropriate technical measures against the unauthorised and unlawful processing of data, as well as against accidental loss, blocking or destruction of processed data. For example, in most cases, any personal data information system (even a simple database) must be certified by FSTEK. In certain cases, such as the processing of large volumes of data or biometric data, the data operator can only use hardware and software for the processing that has been approved by FSTEK or FSS.

21 Notification of data breach

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 PD Law does not expressly require the data operator to notify the authorities of data security breaches. If the request for rectification was made by the affected individual or Roskomnadzor, then the operator has an obligation to notify the affected individual or Roskomnadzor within three days of rectification.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Under article 22.1 of the PD Law, the data operator must appoint a data protection officer. There is no specification whether the officer must be an employee of the data operator under the PD Law. However, Roskomnadzor generally expects the data protection officer to be employed by the data operator. The officer must report directly to the general manager (director) and is responsible for the application of the provisions of the PD Law within the company and other data-related laws, as well as for maintaining a register of data processing operations. In particular, the officer must:

- implement appropriate internal controls over the data operator and its employees;
- make the data operator's employees aware of personal data-related regulations, any internal rules on data protection and other data protection requirements; and
- deal with applications and requests from individuals.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The PD Law requires data operators as well as third-party service providers that process personal data under the operators' instructions to establish a system of internal (local) documents with a detailed description of protective measures taken by such person ('organisational measures' of protection). One of the protective measures involves establishing an internal system of control over access to the personal data processed, which includes keeping records of access to the data. As a general rule, such access to data is granted only for a temporary period and for business needs.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The PD Law does not provide for obligations in relation to new processing operations, such as privacy-by-design approach or privacy impact assessments. Article 18.1 of the PD Law generally obliges operators to regularly conduct internal audits of personal data processing activities for their compliance with the PD Law.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

As a general rule under article 22 of the PD Law, data operators are required to be registered with Roskomnadzor. The PD Law does not specifically regulate whether data processors must be registered with Roskomnadzor. Nevertheless, Roskomnadzor believes that both data operators and data processors must be registered, unless an exemption from the general rule applies.

The registration procedure includes a one-off notification from the data operator to Roskomnadzor. If the data processing characteristics (purposes, terms, third parties having access to the data or other) change, the data operator should notify Roksomnadzor on these changes. Roskomnadzor maintains a public register of data operators. In the absence of any queries, Roskomnadzor acknowledges receipt of the information from the data operator and adds the information on the data operator to the register within 30 days.

There are exceptions from the general rule on the obligatory registration for simple, one-off collections of data and HR-related data. For example, exemptions apply if the data:

- is processed under employment law only;
- is received by the data operator in connection with a contract with the individual, provided that such personal data is not transferred to or circulated among third parties without the individual's consent, and only used either to perform the contract or to enter into further contracts with the individual;
- relates to a certain type of processing by a public association or religious organisation;
- was made publicly available by the individual;
- consists only of the surname, first name and patronymic of the individual; or
- is necessary for granting one-time access to the individual into the premises where the data operator is located and in certain other cases.

26 Formalities

What are the formalities for registration?

The notification form to be filled by the data operator can be found on Roskomnadzor's website at www.pd.rkn.gov.ru, together with guidance on its completion. The information to be provided to Roskomnadzor includes the following:

- the name and address of the data operator;
- the type of data being processed;
- a description of the categories of the data subjects whose data is being processed;
- the purpose of processing;
- the time frame of processing;
- the information on the location of the database with the personal data of Russian citizens; and
- a description of IT systems and security systems used by the data operator.

All of the above information, except for the description of the IT systems and security measures used for the protection of processed data, is made publicly available.

The notification may be submitted electronically on Roskomnadzor's website. However, the data operator must also send a paper version of the notification signed by its general manager (director) to the territorial division of Roskomnadzor. If the information contained in the notification changes (including, eg, the scope of IT systems used by the data operator to process the personal data), the operator must notify Roskomnadzor of such changes within 10 working days of the change. Notification or any further amendment of the entry in Roskomnadzor's register does not require any fee payment by the data operator.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Failure by the data operator to notify Roskomnadzor of data processing is subject to an administrative fine of up to 5,000 roubles under article 19.7 of the Administrative Code. The same administrative penalties are imposed for late submission of the notification or amendments thereto.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Provided that the notification is complete and contains the correct data, Roskomnadzor has no authority to refuse the data operator an entry in the register. Article 22 of the PD Law allows Roskomnadzor to obtain rectification of the information contained in the notification from the data operator before the information is recorded.

29 Public access

Is the register publicly available? How can it be accessed?

The register of data operators is available to a certain extent on Roskomnadzor's website; however, it has limited search capacities. The register contains information on the particulars of data processing by the data operator, except for the description of IT systems and security measures. The information in the register is in Russian only.

30 Effect of registration

Does an entry on the register have any specific legal effect?

The data operator may start processing the data, in accordance with the purposes and methods described in the notification, upon submitting notification to Roskomandzor.

31 Other transparency duties

Are there any other public transparency duties?

Under article 18.1 of the PD Law, an operator is required to publish on its website or otherwise provide unlimited access to its policy describing data processing activities and data protection measures.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under article 6 of the PD Law, the data operator may assign or delegate the processing to a third party, which will act under the instruction of the operator.

There is no statutory form for such instruction by the operator, or for the standard form or precedent of the data transfer agreement approved by Roskomnadzor. The PD Law requires that the instruction of the operator must list the aims of processing, the actions the third party is permitted to perform on the data and the rules of data processing with which the third party must comply (including certain purely technical requirements on data processing).

A third party processing personal data under the operator's instruction must undertake to the operator to maintain the security and confidentiality of the data transferred. As a general rule, assignment of data processing to a third party providing outsourced processing services requires the individual's consent absent an exemption under the PD Law (see question 11).

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Any transfer (including disclosure) of personal data requires the consent of the individual (unless explicitly allowed by the PD Law or other laws). If such consent is obtained by the data operator, there are no restrictions on the disclosure to which consent was given.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Under article 12 of the PD Law, in the event of a cross-border transfer of data, the data operator must check that the data subjects' rights are adequately protected in the foreign country before the transfer. All countries that are party to the European Convention on Personal Data dating from 28 January 1981 are considered to be countries 'having adequate protection of data subjects' interests' (ie, 'safe' countries). Further, Roskomnadzor has approved a list of countries that are not party to the above European Convention but are, nonetheless, considered to be 'safe' countries for the purpose of cross-border transfers (including Qatar, Costa Rica, Singapore, Mali, Gabon, Kazakhstan, Republic of South Africa, Canada, Israel, New Zealand, Mongolia and Peru).

Cross-border transfers of personal data to 'safe' countries are not subject to any specific requirements, provided that the data operator has received consent from the data subject on the transfer of his or her data and issued 'an instruction of a data operator', if needed (see question 32). Data transfers to 'non-safe' countries (eg, Japan and the United States) are allowed only if one of the following requirements is met:

- the subject consented in writing to the cross-border transfer of his or her data;
- the transfer is made under an international treaty of the Russian Federation;
- the transfer is required by applicable laws for the purpose of protecting the constitutional system of the Russian Federation, its national defence or the secure maintenance of its transportation system;
- the transfer is necessary to perform the contract to which the individual is a party or under which he or she is a beneficiary or guarantor; or
- the transfer is needed to protect the individual's life, health or other vital interests and it is impossible to obtain his or her prior consent.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

There is no obligation to notify Roskomnadzor or any other supervisory authority of any data transfer.

Update and trends

Roskomnadzor has announced the beginning of its work on the draft of the 'Infocommunications Code', which is supposed to replace the PD Law and all other laws regulating personal data protection, the use of cloud services and other aspects of 'online activities'. The key purpose of the regulator is to align and update the regulation taking into account the new technologies developed over past 15 years (including the internet, messengers, digital content and cloud services), as well as to provide regulatory flexibility to account for future technology. The text of the Infocommunications Code is not yet publicly available, but reportedly will be presented by the end of 2018.

36 Further transfer

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 data transfers (including cross-border transfers to 'safe' or 'non-safe' countries) are equally applicable to any transfer of data.

Rights of individuals

37 Access

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

Under article 14 of the PD Law, the individual is entitled to request the details of the processing of his or her data from the data operator and access his or her personal data. The data operator may not charge a fee for providing the information or access to the data.

The individual has the right to obtain confirmation on whether his or her personal data is being processed at any time on request to the data operator. The request may also be submitted by a representative of the data subject. There is no statutory form for the request; however, the PD Law requires that it must contain information on the requester's identity (ie, passport details of the data subject or his or her representative) and the information necessary to find the appropriate records (ie, a detailed explanation of the relationship between the data subject and the data operator, including references to the relevant agreement or other arrangements).

If the personal data is being processed by the data operator, the operator has 30 days to respond to the request of the data subject or his or her representative and to provide all of the following information:

- confirmation of the processing of data;
- the legal grounds for and purposes of the processing;
- the purposes and methods of processing;
- the name and address of the data operator and any recipients (other than the data operator's employees) who have access to the personal data or to whom the personal data is to be disclosed under an agreement with the data operator or otherwise as required by law;
- the scope of the personal data processed and the source of the personal data (unless another procedure for receiving personal data is established by a federal law);
- the terms of processing, including the period for which the personal data will be stored;
- the scope of rights of the individual as provided by the PD Law;
- information on any (implemented or planned) cross-border transfers of the personal data;
- if applicable, the name and address of any third-party processor of the personal data acting under 'instruction of the operator'; and
- any other information as required by applicable law.

Article 14 of the PD Law sets out a narrow set of circumstances in which the access rights of the individual may be limited. For example, access may not be provided if the data processing relates to investigative or anti-money laundering activity carried out by state authorities, or if granting access to the information would curtail the rights of other data subjects.

38 Other rights

Do individuals have other substantive rights?

In addition to the right to require access to his or her personal data and request the details of data processing, the data subject may also request the correction of inaccurate data processed by the operator and require the operator to inform any third party with access to the inaccurate data of the corrections made. Further, data subjects are entitled to demand that the data operator discontinue the processing of the personal data (except where the processing cannot be terminated or would result in violations of Russian law, eg, labour law requirements). The data subjects can request the deletion of particular data, if such data is inaccurate, unlawfully obtained or unnecessary for the purpose of processing by the data operator.

39 Compensation

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 article 24 of the PD Law, compensation for any moral damage to an individual resulting from an infringement of his or her rights related to personal data processing and protection must be provided irrespective of any compensation for property damage or other losses. There is no legal interpretation as to what kind of violation of PD Law would lead to an imposition of monetary damages. As a general rule, articles 151 and 1101 of the Civil Code of the Russian Federation require the court to consider the 'degree of guilt' (ie, whether the infringement was gross or merely negligent, and whether there was an element of any intention or malice) and the 'degree of suffering' of the individual. However, compensation for moral damage caused by a violation of the personal data protection rules is rarely applied in practice.

40 Enforcement

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

Article 17 of the PD Law provides that if the data subject discovers a violation of his or her rights by the operator, the data subject is entitled to protect these rights through the authorised body for the protection of data subjects' rights (ie, Roskomnadzor), or in court. Roskomnadzor is entitled to impose administrative penalties on data operators for non-compliance with personal data protection laws, which the data operators may appeal in court.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

There appear to be no further exemptions apart from those described above.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

The orders of Roskomnadzor may be appealed in court. There have been a growing number of appeals by data operators against decisions imposing administrative liability for non-compliance with personal data protection laws.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The use of 'cookies' and equivalent technology on tracking behavioural data is not clearly regulated by Russian law. According to

Roskomnadzor, the use of cookies and equivalent technologies may in certain cases be considered as personal data processing subject to the user's explicit consent.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Unsolicited electronic communications (including via email, fax or telephone) are prohibited. Any data processing for the purpose of direct marketing is allowed only with the prior consent of the data subject. Such consent can be revoked by the data subject at any time, meaning that the data operator is unable to further process personal data. The rules on electronic communications marketing are set out in article 15 of the PD Law and in article 18 of Federal Law No. 38-FZ on Communication (2006).

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Russian law does not specifically regulate the use of cloud computing services. There is also no official guidance on this subject by Roskomnadzor. The use of cloud computing services for storage of personal data will be generally subject to all requirements of the PD Law.

Morgan Lewis

Ksenia Andreeva **ksenia.andreeva@morganlewis.com**
Anastasia Dergacheva **anastasia.dergacheva@morganlewis.com**
Anastasia Kiseleva **anastasia.kiseleva@morganlewis.com**
Vasilisa Strizh **vasilisa.strizh@morganlewis.com**
Brian Zimbler **brian.zimbler@morganlewis.com**

Legend Business Centre
Tsvetnoy Bulvar, 2
Moscow 127051
Russia

Tel: +7 495 212 2500
Fax: +7 495 212 2400
www.morganlewis.com

Serbia

Bogdan Ivanišević and Milica Basta
BDK Advokati

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The Personal Data Protection Act 2008 (DP Act), governs the collection and use of PII. Serbia is not an EU member, but the DP Act has adopted some of the basic principles of the Data Protection Directive.

Sectoral laws also apply to PII processing in particular areas (see questions 6 and 7).

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Serbian data protection authority responsible for overseeing the implementation of the DP Act is the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner).

In the performance of its tasks, the Commissioner has the right to access and examine:

- PII and PII files;
- all documents relating to collection of PII and to other processing activities, as well as to the exercise of the rights of the individual;
- PII owners' general enactments; and
- premises and equipment that the PII owners use.

As a supervisory authority, the Commissioner has the power to supervise PII owners by means of inspections. The inspectors act upon information acquired ex officio or received from complainants or third parties.

3 Legal obligations of data protection authority

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

The Commissioner has an explicit obligation to cooperate with data protection authorities from other countries. The DP Act does not give further details on the manner of cooperation or a mechanism to resolve different approaches.

4 Breaches of data protection

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

Breaches of the DP Act, established in the process of supervision, may result in an issuance of warnings or orders by the Commissioner. When the Commissioner detects a breach, he or she may:

- order the rectification of the irregularity within a specified period of time;
- temporarily ban the processing carried out in breach of the provisions of the DP Act; or
- order deletion of the PII collected without a proper legal basis.

Some of the breaches of law are set out as misdemeanours for which the DP Act prescribes fines. The Commissioner is authorised to initiate misdemeanour proceedings, while misdemeanour courts conduct the proceedings and impose sanctions.

There are also criminal penalties for unauthorised collection of personal information. The penalties are not prescribed in the DP Act, but in the Criminal Code (article 146), and ordinary courts are in charge of imposing them.

Scope

5 Exempt sectors and institutions

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

In general, the DP Act covers all sectors and types of organisation, as well as areas of activity. As a partial exception, the DP Act does not apply to political parties, organisations, trade unions and other forms of associations who process PII pertaining to their members, provided that the member has waived in writing the application of specified provisions of the Act for a specified period of time not exceeding the termination of his or her membership.

In addition, most of the provisions of the DP Act do not apply to journalists and other media operatives when they process PII for the sole purpose of publishing the information in the mass media. The law fully applies, however, to the processing of PII for advertising purposes.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The DP Act is an 'umbrella regulation' in the field of PII protection in Serbia. Therefore the general principles set out in the DP Act apply to all forms of PII processing, including interception of communications, electronic marketing, and monitoring and surveillance of individuals. There are also sectoral laws regulating PII processing in these fields. For example, the Electronic Communications Act 2010 regulates interception of communications, while the E-commerce Act 2009 regulates electronic marketing. Comprehensive regulation of the monitoring and surveillance of individuals is still missing.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

The following laws provide for specific data protection rules:

- Patients' Rights Act 2013 on the obligation of health professionals to keep the patients' PII confidential;
- Labour Act 2005 on PII processing within the employment sector. The law provides for the right of employees to access the PII held

by their employer and to have specific parts of their PII corrected or erased;
- Labour Records Act 1996 on collecting and keeping the PII in the employment sector;
- Healthcare Documentation and Healthcare Records Act 2014 on collecting and keeping the PII in the healthcare sector;
- High Education Act 2017 on PII processing within the sector of higher education;
- Education System Act 2017 on PII processing within the education sector. The processing includes collecting and keeping the PII of pupils, parents, teachers and other employees;
- Pension and Disability Insurance Act 2003 on collecting and keeping PII within the sector of pension and disability insurance;
- Health Insurance Act 2005 on collecting and keeping PII within the health insurance sector; and
- E-Commerce Act 2009, Consumer Protection Act 2014 and Advertising Act 2016 on obtaining consent for direct marketing targeting the consumer.

8 PII formats

What forms of PII are covered by the law?

The DP Act covers all forms of PII. It defines personal data as 'any information relating to a natural person, regardless of the form in which it is manifested or the medium used (paper, tape, film, electronic media, and similar)'.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The DP Act applies to all PII owners, users and processors who process PII in the territory of the Republic of Serbia, regardless of where they have been established or where their seat is.

10 Covered uses of PII

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

The DP Act covers all forms of use or other processing of PII. The Act defines PII processing as any action taken in connection with the information, including: collection, recording, transcription, multiplication, copying, transmission, search, classification, storage, separation, adaptation, modification, making available, use, dissemination, recording, storage, disclosure through transmission or otherwise, dislocation, as well as other actions carried out in connection with the PII, regardless of whether such actions are automated, semi-automated, or carried out otherwise.

There is a statutory distinction between those who own PII and those who process PII on behalf of the owners. The former have the status of 'data controllers' and are entirely responsible for PII. They are in charge of establishing and maintaining PII processing records, notifying the Commissioner of their intent to establish a PII file, registering a PII file with the Central Data Filing System Register, responding to individuals' requests to access the PII, and so on. The latter have the status of 'data processors' and are responsible for processing the entrusted PII properly, in accordance with law or contract provisions, and also for the implementation of adequate security measures.

Legitimate processing of PII

11 Legitimate processing – grounds

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

The processing has to be grounded in either a statutory provision or the data subject's consent. The consent must be given in a proper form (ie, in writing or orally on the record).

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The DP Act has strict requirements concerning the processing of 'particularly sensitive data', defined as PII relating to ethnicity, race, gender, language, religion, political party affiliation, trade union membership, health status, receipt of social support, status of a victim of violence, criminal record and sex life. Only the data subject's consent may constitute legal basis for the processing of particularly sensitive PII. The form of the consent, as prescribed by the DP Act, is more stringent than the form of consent for the processing of other types of PII. Exceptionally, PII relating to political party affiliation, health status or receipt of social support may be processed without consent, if a law permits it. Processing of particularly sensitive PII must be specially marked and protected by safeguards.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The PII owner has to inform individuals on all relevant aspects of the PII processing. The notice, as a rule, has to be provided before the PII is collected and has to contain information about:
- the name and address or business name of the PII owner or the identity of another person responsible for PII processing (if any);
- the purpose of PII collection and the subsequent processing;
- the manner in which the PII will be used;
- the identity or categories of the users of the PII;
- the mandatory nature of, and the legal basis for, the processing; or, conversely, the voluntary nature of providing the PII;
- the individual's right to withdraw his or her consent to the processing and the legal consequences in the event of a withdrawal (the individual should compensate the PII owner for any reasonable costs and damages caused by the withdrawal);
- the individual's rights in the case of unlawful processing (eg, the right to request deletion of PII and suspension of the processing); and
- any other information, which, if withheld, could be considered contrary to 'conscientious practice'.

In addition, a PII owner who collects PII from a third party must inform the individual about it, without delay and in any event no later than at the time of the first processing.

14 Exemption from notification

When is notice not required?

Notice is not required when giving a notice would be impossible, evidently unnecessary, or unsuitable, especially if the individual has already been informed or the individual is unavailable. The Commissioner has provided little guidance on this issue.

When a PII owner collects PII from a third party, notice to the individual is not required if notification is impossible, unnecessary, or requires excessive use of time or efforts. Examples of when notification is unnecessary include the following:
- the individual has been already informed;
- the individual is unavailable; and
- a law provides for collection and processing of the PII obtained from a third party.

However, even in these cases the PII owner must notify the individual as soon as reasonably possible or, if the notification was evidently unnecessary, at the data subject's request.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Individuals may control use of their PII by not consenting to the PII processing, as well as by exercising the right to access their personal information held by PII owners and other substantive rights (rectification, modification, update and deletion of PII) (see questions 37 and 38).

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The DP Act prescribes in a general manner that the processing of PII is impermissible if the information is inaccurate or incomplete, or if it is not based on a credible source or is out of date.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The DP Act sets forth as one of its main principles that the amount of PII that may be processed has to be proportionate to the purpose of the processing. The Act does not prescribe any particular length of time during which the PII may be lawfully held, but the law indirectly imposes limits on the duration by forbidding further processing if the purpose of the processing has been modified or achieved.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The DP Act adopts the 'finality principle': the purpose of the processing of PII has to be clearly determined and permissible. As a rule, processing for the purposes other than those specified is not allowed.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Personal information collected and processed for a particular purpose may also be processed for historical, statistical, or research and development purposes. In that case, the information has to be properly secured and cannot be used as a basis for rendering decisions or taking measures against the individual.

Security

20 Security obligations

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

The DP Act does not impose specific obligations on PII owners and other processors concerning data security, but provides for their general duty to undertake proper 'technical, human resources, and organisational measures to protect the data in accordance with established standards and procedures in order to protect data from loss, damage, inadmissible access, modification, publication and any other abuse'.

The DP Act stipulates that the government should enact a decree specifying protection measures for particularly sensitive PII. In the nine years since the implementation of the law, the government has not adopted such an act.

21 Notification of data breach

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 DP Act does not require PII owners to notify the Commissioner or the affected individuals of a data breach. The Commissioner has not issued any guidance in relation to this matter. The Electronic Communications Act (2010, as amended) states that an 'operator' (a person or entity carrying out or authorised to carry out electronic communications activities) must notify the Regulatory Agency for Electronic Communications and Postal Services of any breach of security and integrity of public communication networks or services affecting the operator's work, and especially of breaches that undermine the protection of personal data or impinge on subscribers' or users' right to privacy.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The appointment of a data protection officer is not mandatory.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

PII owners are required to establish and maintain PII processing records that contain relevant information on the categories of the PII, name of the PII file, types of the processing activities, purpose of the processing, among others. PII owners do not have to maintain such records if:

- PII is processed solely for family or other personal purposes and is unavailable to the third parties;
- PII is processed for the purpose of maintaining registers required by law;
- the PII file contains publicly available PII only; or
- PII relates to persons whose identity is not determined and the PII owner, processor or user is not authorised to determine such person's identity.

The Decree on the Form and Manner of Keeping Records of Personal Data Processing lays down the rules on the form that the processing records should take.

PII processors are not required to maintain internal records or establish internal processes or documentation.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The only obligation in relation to new processing operations is to notify the Commissioner of the intended processing, so that the Commissioner may conduct a prior checking procedure and determine whether the processing would entail specific and significant risk for the rights and freedoms of data subjects. The data controller may not commence the processing operations until the prior checking procedure has been completed with the issuance of the Commissioner's approval.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

PII owners are required to notify the Commissioner of the intended processing of PII, as well as to register with the Commissioner the PII processing records (filing systems) and any subsequent change in the records. The Commissioner maintains the Central Data Filing Systems Register, which includes both the notifications and the PII processing records. The obligation to notify about the intended processing does not exist if a specific law determines the purpose of the processing, the categories of PII to be processed, the categories of users of the PII, and the period during which the PII will be held. In contrast, there are no exceptions to the obligation to register the PII processing records. PII processors do not have an obligation to register with the supervisory authority.

26 Formalities

What are the formalities for registration?

When PII owners submit to the Commissioner the PII processing records, the records have to include the information referred to in the response to question 23 (categories of PII, name of the PII file, types of processing activities, purpose of the processing, and other information).

There is no payable fee for registration. Registration is valid for an indefinite period of time, so it does not have to be periodically renewed.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Under the DP Act, failure of the PII owner to register a data filing system or changes in the system within the required 15-day period constitutes a misdemeanour. The fine ranges from 50,000 to 1 million Serbian dinars for PII owners with the status of legal entities, and from 20,000 to 500,000 Serbian dinars for entrepreneurs. The fine for a natural person is 5,000 to 50,000 Serbian dinars. The same penalty applies to the responsible officer of a legal entity, state agency, or a governing body of the territorial autonomy or local self-government.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The Commissioner may decide, when reviewing the notification files, that conditions for a lawful processing of PII are not met owing to a lack of statutory basis for the processing or lack of consent, impermissible or undetermined purpose, impermissible means of processing, inadequacy of the PII for the achievement of the purpose, disproportionate amount or categories of the PII, or non-truthfulness or incompleteness of the information. If the prior checking results in a positive finding, the Commissioner has to allow an entry on the register.

29 Public access

Is the register publicly available? How can it be accessed?

The Central Data Filing System Register is publicly available on the official site of the Commissioner, at www.poverenik.rs/registar/index.php?lang=yu. The information on the site is in Serbian only. Upon request of the PII owner, the Commissioner may deny general access to the details about the filing system, if this is necessary for the achievement of a prevailing interest of national or public safety, national defence, performance of tasks by public authorities, or financial interests of the state, or if a law or other type of regulation provides for confidentiality of the information in the filing system.

30 Effect of registration

Does an entry on the register have any specific legal effect?

The main purpose of an entry on the Central Data Filing Systems Register is to ensure transparency of the PII processing. That is, to make the information about the filing systems and the PII owners available to the general public.

31 Other transparency duties

Are there any other public transparency duties?

There are no other public transparency duties.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

There are no specific provisions regulating the transfer of PII to entities providing processing services to the PII owners. Under the DP Act, 'data processor' is a subject to whom the PII owner delegates certain processing-related activities on the basis of a law or contract.

Update and trends

The DP Act is in the process of being changed. The new Act will mirror the provisions of the GDPR, as Serbia is a candidate for membership of the EU. The Ministry of Justice prepared the new Act in November 2017, and Parliament is expected to adopt a new law by the end of 2018.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

PII owners may disclose the PII to other recipients (PII users) only on the basis of a statutory provision or consent of the data subject. The purpose of the disclosure must be legitimate.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The cross-border transfer of PII from the Republic of Serbia to a country that is party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) is not restricted nor subject to any authorisation. In a case of this kind, lawful processing of PII is the sole condition that PII owners have to meet in order to transfer the information lawfully. On the other hand, for cross-border transfer to countries that are not parties to Convention 108 and to international organisations, it is necessary to obtain prior approval from the Commissioner.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Prior approval from the Commissioner is necessary for cross-border transfers of PII to countries not parties to Convention 108 and to international organisations. In such cases, PII owners have to submit requests to the Commissioner, designating the PII filing systems they intend to transfer, the countries or international organisations to whom they want to transfer the PII, the identity of the subject abroad to whom they want to transfer the PII, and other relevant information about the transfer. The PII owners also have to submit copies of the transfer agreements with the importers. The Commissioner then assesses the safeguard measures and other relevant circumstances of the intended transfer, and issues a decision. The procedure may take any time from a few months to one year, or even more.

36 Further transfer

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 specific provisions regulating further transfers of PII. However, according to the recent practice of the Commissioner, such transfers do not require prior approvals.

Rights of individuals

37 Access

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

Individuals have the right to be accurately and fully informed about the processing of their PII, the right to access the PII and the right to obtain a copy of the PII. In order to exercise these rights, the individual must submit a request to the PII owner, in the form prescribed by the DP Act. Restrictions on the enjoyment of the rights include the situation in which the individual requests information pertaining to the PII already in the public domain, whether in public registers or otherwise, and the situation in which the individual abuses his or her rights.

38 Other rights

Do individuals have other substantive rights?

Upon obtaining access to the PII, individuals have the right to require from the PII owners to correct, modify, update or delete the PII. They also may require suspension of the processing.

Individuals have the right to require deletion of their PII when:

- the purpose of the processing is not clearly specified;
- the purpose of the processing has changed and requirements for processing with the different purposes are not met;
- the purpose of the processing has been achieved or the PII is no longer needed for such purpose;
- the PII is processed by impermissible means;
- the scope or type of the PII processed is disproportionate to the purpose of the processing;
- the PII is inaccurate and it is not possible under the circumstances to replace it with accurate PII by means of a correction; or
- the PII is processed without consent or statutory authorisation.

Individuals may obtain suspension of the processing if they successfully contest how accurate, complete or up to date the PII is. Pending a decision on the challenge, individuals may obtain designation of such PII as contested.

39 Compensation

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 Obligations Act (1978), which contains general provisions on indemnity for torts, individuals are entitled to compensation of damage caused by violations of their right to protection of PII. PII owners may be liable both for actual damage and for moral damage (injury to feelings).

40 Enforcement

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

If the PII owner rejects or denies the individual's request for exercising his or her rights, fails to decide on a request within the specified time limit, as well as in other cases prescribed by the DP Act, the individual may lodge a complaint with the Commissioner. The Commissioner issues a ruling, which may be challenged in administrative proceedings before the Administrative Court.

Damages must be brought to a civil court.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Not applicable.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

PII owners can appeal to the Administrative Court against orders of the Commissioner.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The Electronic Communications Act provides that the PII owner can store cookies on the individual's terminal equipment if the individual is provided with clear and comprehensive information about the purpose of the collection and processing of PII and given an opportunity to refuse such processing.

There have been no authoritative rulings by the Commissioner or the courts as to adequacy of the specific modes of cookie notification.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

The E-commerce Act 2009 states that unsolicited commercial messages may be sent via email to individuals only if individuals have given their prior consent to such types of marketing.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific provisions in the legal system of the Republic of Serbia regulating cloud computing services.

BDK Advokati
Belgrade • Podgorica • Banja Luka

Bogdan Ivanišević **bogdan.ivanisevic@bdkadvokati.com**
Milica Basta **milica.basta@bdkadvokati.com**

Bulevar kralja Aleksandra 28
Belgrade 11000
Serbia

Tel: +381 11 3284 212
Fax: +381 11 3284 213
www.bdkadvokati.com

Singapore

Lim Chong Kin
Drew & Napier LLC

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Prior to the enactment of the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA), Singapore did not have an overarching law governing the protection of personally identifiable information. 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 will continue to operate alongside the PDPA.

The PDPA was implemented in three phases. On 2 January 2013, selected provisions of the PDPA came into operation. These include provisions that:

- set out the scope and interpretation of the PDPA;
- provide for the establishment of the Personal Data Protection Commission (PDPC) and the Data Protection Advisory Committee (DPAC); and
- provide for the establishment of Do-Not-Call (DNC) registers by the PDPC, and other general provisions of the PDPA.

On 2 January 2014, provisions relating to the DNC registry came into force; and the main data protection provisions under parts III to VI of the PDPA came into effect on 2 July 2014. The main data protection provisions set out the obligations of organisations with respect to the collection, use, disclosure, access to, correction and care of personal data.

Regulations and advisory guidelines under the PDPA deal with specific issues in greater detail.

The Personal Data Protection Regulations 2014 (the PDP Regulations) were gazetted on 19 May 2014. The PDP Regulations supplement the PDPA in three key areas as follows:

- the requirements for transfers of personal data out of Singapore;
- 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 in relation to disclosure of personal data of deceased individuals.

The other regulations issued under the PDPA are:

- Personal Data Protection (Composition of Offences) Regulations 2013;
- Personal Data Protection (Do Not Call Registry) Regulations 2013;
- Personal Data Protection (Enforcement) Regulations 2014; and
- Personal Data Protection (Appeal) Regulations 2015.

In addition, the PDPC has issued a number of advisory guidelines to provide greater clarity on the interpretation of the PDPA, namely:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Key Concepts Guidelines);
- Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Selected Topics Guidelines);
- Advisory Guidelines on the Do Not Call Provisions;
- Advisory Guidelines for the Telecommunication Sector;
- Advisory Guidelines for the Real Estate Agency Sector;
- Advisory Guidelines for the Education Sector;
- Advisory Guidelines for the Healthcare Sector;
- Advisory Guidelines for the Social Service Sector;
- Advisory Guidelines on Requiring Consent for Marketing Purposes (Marketing Consent Guidelines);
- Advisory Guidelines on Enforcement of Data Protection Provisions (Enforcement Guidelines);
- Advisory Guidelines on Application of PDPA to Election Activities; and
- Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire.

The PDPC has further published general guides to supplement the regulations and guidelines above, which include:

- Guide to Notification;
- Guide to Managing Data Breaches;
- Guide to Securing Personal Data in Electronic Medium;
- Guide on the Practice of Passing Magnetic Stripes of Payment Cards Through a Reader;
- Guide to Handling Access Requests (Access Requests Guide);
- Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data;
- Guide on Building Websites for SMEs;
- Guide to Disposal of Personal Data on Physical Medium;
- Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data;
- Guide to Data Sharing;
- Guide to Developing a Data Management Programme;
- Guide to Data Protection Impact Assessments (DPIA Guide);
- Guide to Basic Data Anonymisation Techniques; and
- Guide to Printing Processes for Organisations.

The PDPC has also provided comments and suggestions to the following industry-led guidelines on the PDPA that were developed by the Life Insurance Association Singapore (the LIA) and published on 1 April 2015:

- LIA Code of Practice for Life Insurers on the Singapore Personal Data Protection Act; and
- LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act.

In 2017, the PDPC published its inaugural Personal Data Protection Digest, which is a compendium comprising the PDPC's grounds of decisions released since 2016, summaries of unpublished cases where a finding of no-breach was found and a collection of data protection-related articles contributed by data protection practitioners. The Personal Data Protection Digest is available on the PDPC's website.

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 OECD Guidelines

on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework, in developing the PDPA framework.

The PDPC is currently undertaking a review of the PDPA, and has held two public consultations in this regard. First, the Public Consultation for Approaches to Managing Personal Data in the Digital Economy (issued 27 July 2017) sought the public's views on introducing:

- a Proposed Enhanced Framework for the Collection, Use and Disclosure of Personal Data; and
- a Proposed Mandatory Data Breach Notification Requirement.

Second, the Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (issued 27 April 2018) sought the public's views on:

- streamlining the DNC provisions in Part IX of the PDPA and the Spam Control Act into a single legislation governing all unsolicited commercial messages;
- introducing an Enhanced Practical Guidance framework under the PDPA, which allows the PDPC to provide guidance to organisations with greater clarity and certainty; and
- streamlining the exceptions to obtaining consent for the collection, use and disclosure of personal data, found in the Second, Third and Fourth Schedules to the PDPA. The consultation closed on 12 June 2018.

On 20 February 2018, Singapore became the sixth APEC economy to participate in the APEC Cross-Border Privacy Rules (CBPR) system, along with the USA, Mexico, Canada, Japan and the Republic of Korea. 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 PDPC is currently developing the certification scheme for the CBPR and PRP systems and, in March 2018, called for interested companies to act as assessment bodies for its Data Protection Trustmark Certification scheme. Once the certification scheme is implemented, organisations may start applying for certification under the relevant systems.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The PDPA is administered and enforced by the PDPC. The PDPC was originally established as a statutory body under the PDPA on 2 January 2013 and was under the purview of the Ministry of Communications and Information (the MCI). With effect from 1 October 2016, the PDPC has been subsumed as a department/division under the Info-communications Media Development Authority (IMDA). The leadership team of the PDPC comprises:

- Mr Tan Kiat How, commissioner, the PDPC;
- Mr Leong Keng Thai, executive chairman of the Data Protection Advisory Committee; and
- Mr Yeong Zee Kin, deputy commissioner, the PDPC.

The PDPC may initiate an investigation to determine whether an organisation is compliant with the PDPA, upon receipt of a complaint or of its own motion. As set out in the Enforcement Guidelines, the factors that the PDPC may consider in deciding whether to commence an investigation include:

- whether the organisation may have failed to comply 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;
- whether the complainant had previously approached the organisation to seek a resolution of the issues in the complainant but failed to reach a resolution;
- where the PDPC has sought to facilitate dispute resolution between the complainant and the organisation, whether the complainant and the organisation agreed to participate in the dispute resolution process and their conduct during the dispute resolution process and the outcome of the dispute resolution process;
- where the PDPC has commenced a review, whether the organisation has complied with its obligations under the Enforcement Regulations in relation to a review, the organisation's conduct during the review and the outcome of the review;
- public interest considerations; and
- any other factor that, in the PDPC's view, indicates that an investigation should or should not be commenced.

In the course of its investigation, the PDPC is empowered to:

- by notice in writing, require any organisation to produce any specified document or to provide any specified information;
- by giving at least two working days' advance notice of intended entry, enter an organisation's premises without a warrant; and
- obtain 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 in relation to access and correction requests (see questions 37 and 38 for more information on access and correction requests).

The PDPA also establishes the DPAC, 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. Currently, the Advisory Committee is headed by Mr Leong Keng Thai, who is also the Deputy Chief Executive Officer of the IMDA. Under him are 13 other members, namely:

- Professor Simon Chesterman, Dean, Faculty of Law, National University of Singapore;
- Mr Hui Choon Kuen, Deputy Chief Counsel Advisory (Civil Division), Attorney General's Chamber and Dean, AGC Academy;
- Ms Tina Hung, Deputy Chief Executive Officer, National Council of Social Service;
- Mr Mohamed Nasser Ismail, Senior Vice President, Head of Equity Capital Market (SMEs) and Head of Capital Market Development, Singapore Stock Exchange;
- Mr Lam Chee Kin, Managing Director & Head, Group Legal Compliance & Secretariat, DBS Bank Ltd;
- Mr Lim Biow Chuan, President, Consumers Association of Singapore;
- Mr Lim Chin Hu, Managing Partner, Stream Global;
- Associate Professor Low Cheng Ooi, Chief Medical Informatics Officer, Ministry of Health and MOH Holdings;
- Professor Steven Miller; Vice Provost (Research), Singapore Management University;
- Ms Ong Seok Leng, Senior Director (Governance Group), Government Technology Agency;
- Mr Teo Chin Hock, Deputy Chief Executive, Cyber Security Agency;
- Mr Lu Cheng Yang, Secretary General Designate, Singapore Chinese Chamber of Commerce and Industry; and
- Mr Kurt Wee, President, Association of Small and Medium Enterprises (ASME).

The addition of members from the banking, healthcare, IT, public and social services sectors and academia is intended to contribute perspectives from each sector to the Advisory Committee.

3 Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with 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 co-operation 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 in relation to a matter in circumstances where it is satisfied that the other is performing functions in relation to that matter.

Under the PDPA, the PDPC may only furnish information to a foreign data protection body pursuant to a cooperation agreement if it requires of and obtains from that body an undertaking in writing by it that it will comply with terms specified in that requirement, 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 body if the following conditions are specified:

- the information or documents requested by the foreign data protection body are in the possession of the PDPC;
- the foreign data protection body 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 (section 59(5) of the PDPA).

The PDPC is also a participant to 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.

4 Breaches of data protection

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;
- powers relating to review applications; and
- powers of investigation.

Any individual affected by an organisation's non-compliance with any of the main 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. As mentioned in question 2, the PDPC may commence an investigation in respect of potential breaches of the PDPA further to a complaint, or on its own motion.

In this regard, the Enforcement Guidelines and the public guidance published on the PDPC's website as of June 2018 states that, when a complaint is received by the PDPC, the PDPC may assess if it can help to address the individual's concerns by facilitating communications between the individual and the organisation.

If the individual and the organisation are unable to resolve the matter directly and require additional assistance, the PDPC may refer the matter for mediation by a qualified mediator where both the complainant and the organisation involved have consented to the same.

That said, where the PDPC is satisfied that an organisation has breached the main data protection provisions under the PDPA, it is empowered with a 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 or correct personal data, or reduce or make a refund of any fee charged for any access or correction request; or
- pay a financial penalty of up to S$1 million.

In calculating a financial penalty, the PDPC may consider any applicable aggravating or mitigating factors. According to the Enforcement Guidelines and the public guidance published on the PDPC's website as of June 2018, some of the factors that the PDPC may consider to be aggravating factors include:

- the organisation failing to actively resolve the matter with the individual in an effective and prompt manner;
- intentional, repeated or ongoing breaches of the data protection provisions by an organisation;
- obstructing the PDPC during the course of investigations (such as making efforts to withhold or conceal information requested by the PDPC);
- failing to comply with a previous warning or direction from the PDPC; and
- the organisation is in the business of handling large volumes of sensitive personal data (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of that personal data.

Some of the factors that the PDPC may consider to be mitigating factors include:

- the organisation's active and prompt resolution of the matter with the individual;
- the organisation taking reasonable steps to prevent or reduce the harm of a breach (such as putting in place strong passwords or encrypting the personal data to prevent unauthorised access);
- the individual affected by the breach has already received a remedy in some other form (for example, through a civil action against the organisation);
- the organisation engaging with the individual in a meaningful manner and having voluntarily offered a remedy to the individual, and that individual having accepted the remedy;
- the organisation taking immediate steps to notify affected individuals of the breach and reduce the damage caused by a breach (such as informing individuals of steps they can take to mitigate risk); and
- the organisation voluntarily notifying the personal data breach to the PDPC as soon as it learned of the breach, and cooperating with the PDPC in its investigations.

On 21 April 2016, the PDPC announced that it had taken its first batch of enforcement actions against 11 organisations for breaching their data protection obligations under the PDPA. Five organisations were issued directions (four of which included financial penalties), while six others were issued warnings. Notably, 10 out of 11 organisations were found to have failed to implement reasonable security arrangements to protect personal data under their possession or control. Since then, the PDPC has also published further enforcement actions taken against organisations that have breached their data protection obligations.

Any person who suffers loss or damage directly as a result of a contravention of any of the main data protection provisions may also commence a private civil action in respect of such loss or damage suffered (see question 38 for further information on such right of private action).

Non-compliance with certain provisions under the PDPA may also constitute an offence, for which a fine or a term of imprisonment may

be imposed. The quantum of the fine and the length of imprisonment (if any) vary, depending on which provisions are breached. For instance, a person found guilty of making requests to obtain access to or correct the personal data of another without authority may be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding 12 months, or both. Intentionally disposing of, altering, falsifying, concealing or destroying a record containing personal data or information about the collection, use or disclosure of personal data is an offence that may be punishable upon conviction with, in the case of an individual, a fine of up to S$5,000, and in the case of an organisation, a fine of up to S$50,000. The obstruction of PDPC officers (eg, in the course of their investigations) or provision of false statements to the PDPC may be punishable upon conviction with, in the case of an individual, a fine of up to S$10,000 or imprisonment for a term not exceeding 12 months; and in the case of an organisation, a fine of up to S$100,000. See question 27 for more circumstances under which criminal sanctions may be imposed under the PDPA.

Scope

5 Exempt sectors and institutions

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

The 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 PDPA, such as:

- individuals acting in a personal or domestic capacity;
- employees acting in the course of their employment with an organisation; and
- public agencies, or organisations acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.

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 new 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. For example, the banking secrecy laws under the Banking Act (Cap. 19) still govern customer information obtained by a bank, and the Telecom Competition Code still governs end-user service information obtained by a telecoms licensee.

The PDPC has also published a number of sector-specific advisory guidelines to provide greater clarity on the interpretation of the PDPA in various sectors (see question 1).

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Interception of communications and monitoring and surveillance of individuals

To the extent that personal data is collected in the interception of communications and in the monitoring and surveillance of individuals, the PDPA applies to the organisation collecting such data. As such, the individual's consent has to be sought before any such collection takes place, unless such consent is not required (see question 11 for more information on the consent requirement and its exceptions).

For example, the Selected Topics Guidelines indicate that an employer may not need to seek consent for any personal data collected from its monitoring of its employees' use of company computer network resources as long as such collection is reasonable for the purpose of managing or terminating the employment relationship, although under section 20(4) of the PDPA, it is still required to notify its employees of this purpose for such collection of their personal data.

In relation to CCTV surveillance, the Selected Topics Guidelines explicitly clarify that organisations that install CCTVs in their premises are required to put up notices informing individuals that CCTVs are operating in the premises, stating the use and purpose of such surveillance, and if both audio and video recordings are taking place, to state as such, to fulfil their obligation to obtain consent for the collection, use or disclosure of personal data from CCTV footage. This is unless such consent is not required, for example, if the CCTV surveillance is necessary for any investigation or proceedings, insofar as it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data. Moreover, the PDPC recommends that while such notices should be placed at points of entry or prominent locations in a venue or a vehicle to enable individuals to have sufficient awareness that CCTV has been deployed in the general locale, they do not have to reveal the exact location of the CCTV cameras. The PDPC also clarifies that an individual may request access to CCTV footage containing his or her image in accordance with the PDPA, unless an exception to this right applies (see question 37 for more details on an individual's right to access his or her personal data and its limitations). However, the PDPC has also indicated that organisations are generally required to provide access to CCTV footage where the images of other individuals present in the CCTV footage are masked as required (assuming that consent from the other individuals for the disclosure of their personal data has not been obtained).

In addition, where the organisations collecting such personal data via the interception of communications or the performance of surveillance or monitoring activities are public agencies (eg, the Singapore Police Force or the IMDA), they are excluded from the application of the PDPA under section 4(1)(c) of the PDPA. Thus, to the extent that the above exceptions apply, the organisation collecting personal data via interception of communication or monitoring and surveillance of individuals will not have to seek the individuals' consent prior to such collection.

Apart from the PDPA, there are other regulations that allow for the interception of communications and the monitoring and surveillance of individuals. Below is a non-exhaustive list of such regulations:

- 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 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 by the [IMDA] or such other relevant law enforcement or security agencies in order to carry out their respective 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 for the police investigation) 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, inter alia, 'intercept any message transmitted or received by telecommunication' or 'intercept or listen to any conversation by telephone'.
- Section 15A of the Computer Misuse and Cybersecurity Act (Cap. 50A) states that the Minister may authorise or direct any person or organisation to, inter alia, 'provid[e] to the Minister or a public officer authorised by him any information (including real-time information) obtained from any computer'. However, upon the coming into force of the Cybersecurity Act 2018 (No. 9 of 2018) on a date yet to be announced, section 15A of the Computer Misuse and Cybersecurity Act will be repealed and replaced with section 23 of the Cybersecurity Act, which provides for the same. The Computer Misuse and Cybersecurity Act will also be renamed the Computer Misuse Act.

Electronic marketing

Section 11 of the Spam Control Act requires any person who 'sends, causes to be sent or authorises the sending of unsolicited commercial

electronic messages (which include both emails and SMS/MMS) 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).

In addition to the requirements under the Spam Control Act regarding the sending of spam messages, the PDPA would also apply to personal data collected, used or disclosed through the use of such electronic marketing. Generally, the PDPA requires organisations to obtain consent for a stated purpose to collect, use or disclose the contact information of individuals, unless any exception applies.

With that said, the PDPC is proposing to review, streamline and merge the DNC provisions of the PDPA and the Spam Control Act into a single legislation governing all unsolicited commercial messages, and is currently seeking comments on this as part of its Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (see question 1).

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Various other legislation in Singapore sets out specific data protection rules, some of which are sector-specific. For instance:

- the Banking Act proscribes the disclosure of customer information by a bank or its officers;
- the Computer Misuse and Cybersecurity Act (which will be renamed the Computer Misuse Act upon the coming into force of the Cybersecurity Act) 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 Electronic Transactions Act (Cap. 88) provides for the security and use of electronic transactions by criminalising any disclosure of electronic data obtained pursuant to the Act, unless the disclosure is expressly allowed under the Act, required by any written law, or mandated by an order of court;
- the Income Tax Act (Cap. 134) contains provisions that prohibit any person who owns or has control over any documents, information, returns, assessment lists or copies of such lists, to disclose or allow others to have access to such information;
- the Payroll Tax Act (Cap. 223) contains provisions that prohibit any disclosure of information relating to remuneration, payroll tax and income tax;
- 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 Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap. 319) details provisions protecting the secrecy of information of statutory bodies and government companies; and
- the Telecom Competition Code issued under the Telecommunications Act (Cap. 323) contains certain provisions pertaining to the safeguarding of end-user service information. Notably, the IMDA has introduced amendments to the provisions governing end-user service information in the Telecom Competition Code effective 2 July 2014, taking into account that the PDPA will be the primary legislation governing personal data.

On 2 June 2014, the Monetary Authority of Singapore (MAS) also issued its Consultation Paper on the Obligations of Financial Institutions under the Personal Data Protection Act 2012 – Amendments to Notices on Prevention of Money Laundering and Countering the Financing of Terrorism (AML/CFT), which set out its proposed amendments to the MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism. The proposed amendments sought to clarify the objections of financial institutions (FIs) under the AML/CFT requirements in relation to the PDPA. Accordingly, these proposed amendments were incorporated into notices issued by the MAS, pertaining to different classes of FIs, which took effect on 1 July 2014. These amendments apply to the following classes of FIs:

- holders of stored value facilities;
- trust companies;
- approved trustees;
- capital markets intermediaries;
- financial advisers;
- life insurers;
- holders of money-changer's licence and remittance licence;
- finance companies;
- merchant banks; and
- commercial banks.

Broadly, they make clear that FIs may continue the existing practice of collecting, using and disclosing personal data without customer consent for the purposes of meeting the AML/CFT requirements, and acknowledge customers' rights under the PDPA to access and correct personal data that is in the possession or under the control of the FI.

8 PII formats

What forms of PII are covered by the law?

All formats of 'personal data' 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.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Data protection provisions

The data protection provisions under the PDPA generally 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 so long as they collect, use or disclose personal data in Singapore. In addition, organisations that collect personal data overseas and host or process it in Singapore will generally also be subject to the relevant obligations under the PDPA from the point that such data is brought into Singapore.

Do-not-call provisions

Similarly, the DNC provisions under the PDPA apply to all individuals and organisations sending marketing messages to Singapore telephone numbers, as long as either the sender (when the marketing message is sent) or the recipient (when the marketing message is accessed) is present in Singapore. As an example of its application, the requirement to check the DNC registers would not apply to overseas telecoms service operators sending marketing messages to Singapore subscribers roaming on overseas telecoms networks, because these messages would not be sent or accessed in Singapore. However, organisations in Singapore that outsource their telemarketing activities to overseas organisations and authorise the sending of marketing messages should note that they are still responsible for complying with the DNC provisions, as section 36(1) of the PDPA defines a sender to include a person who causes the message or a voice call containing the message to be sent, or authorises the sending of the message or the making of a voice call containing the message.

For completeness, as mentioned above, the PDPC is proposing to review, streamline and merge the DNC provisions of the PDPA and the Spam Control Act into a single legislation governing all unsolicited commercial messages, and is currently seeking comments on this as part of its Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (see question 1).

10 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII 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 principal organisation) pursuant to a written contract. A data intermediary is only required to comply with the rules relating to the protection and retention of personal data (see question 32 for further details), while the principal organisation is subject to the full suite of data protection provisions under the PDPA as if it were processing the personal data itself.

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 PII

11 Legitimate processing – grounds

Does the law require that the holding of PII 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 is expressed in terms of 'collection, use and disclosure' of the same under the 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. Fresh consent would need to be obtained where personal data collected is to be used for a different purpose to which the individual originally consented.

In addition, organisations should note that 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, in order 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 where the following conditions are satisfied:

- 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.

Where an individual has given (or is deemed to have given) consent for the disclosure of his or her personal data by Organisation A to Organisation B for a particular purpose, such individual would also be deemed to have given consent to Organisation B for the collection, use or disclosure of his or her personal data for that particular purpose.

While consent is generally needed, the Second, Third and Fourth Schedules to the PDPA provide for specific situations where personal data can be collected, used or disclosed without the individual's consent.

The Second Schedule to the PDPA allows personal data to be collected without consent, for example, where:

- the collection of personal data is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
- the personal data is publicly available;
- the collection of personal data is necessary for any investigation or proceedings, and if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;
- the collection of personal data is for the purpose of recovery of a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;
- the collection of personal data is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services;
- the personal data is included in a document produced in the course of, and for the purposes of, the individual's employment, business or profession and collected for the purposes consistent with the purposes for which the document was produced; or
- the personal data is collected by an individual's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organisation and the individual.

The Third Schedule to the PDPA allows personal data to be used without consent, for example, where:

- the use is necessary for any purpose that is clearly in the interests of the individual and:
  - if consent for its use cannot be obtained in a timely way; or
  - the individual would not reasonably be expected to withhold consent;
- the personal data is publicly available;
- the use is necessary for any investigation or proceedings;
- the personal data is used for an organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation; or
- the use is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services.

The Fourth Schedule to the PDPA allows personal data to be disclosed without consent, for example, where:

- the disclosure is necessary for any purpose that is clearly in the interests of the individual if consent for its disclosure cannot be obtained in a timely way;
- the personal data is publicly available;
- the disclosure is necessary for any investigation or proceedings;
- the disclosure is necessary for an organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;
- the disclosure is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services; or
- the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

In its Public Consultation on Approaches to Managing Personal Data in the Digital Economy, the PDPC has proposed two new bases for organisations to collect, use or disclose personal data without the need for consent; namely, 'notification of purpose' and 'legitimate interests'.

First, the PDPC has proposed to introduce 'notification of purpose' as a basis to collect, use or disclose personal data under the PDPA

without consent, where the collection, use or disclosure of personal data is not expected to have any adverse impact on the individual. Organisations that wish to rely on this basis must provide the individual with appropriate notification of the purpose of the collection, use or disclosure of the personal data, and information about how the individual may opt out, where applicable. Also, organisations must conduct a risk and impact assessment, such as a data protection impact assessment, as an accountability measure to identify and mitigate any risks when seeking to rely on the 'notification of purpose' basis.

Second, the PDPC has proposed to enable organisations to collect, use or disclose personal data without consent in circumstances where there is a need to protect legitimate interests that will have economic, social, security or other benefits for the public (or a section thereof). Such benefits to the public must outweigh any adverse impact to the individual, and organisations wishing to rely on this 'legitimate interests' basis must conduct a risk and impact assessment to determine this is the case. As an additional safeguard, the PDPC intends to provide for an openness requirement whereby organisations relying on 'legitimate interests' as a basis to collect, use or disclose personal data must:

- disclose its reliance on 'legitimate interests' as a ground for collection, use or disclosure (eg, through the organisation's data protection policy that is made available to the public); and
- make available a document justifying the organisation's reliance on 'legitimate interests' and the business contact information of the person who is able to answer individuals' questions about such collection, use or disclosure on behalf of the organisation.

The PDPC published its response to the public consultation on 1 February 2018, and it is expected that the proposed changes will be implemented in due course.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Generally, the PDPA does not distinguish between the types and sensitivities of personal data. However, section 24 of the PDPA requires that an organisation would need to make 'reasonable security arrangements' to protect, and to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to personal data in its possession or under its control. 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 (see question 20).

Certain types of personal data are also accorded less stringent rules under the PDPA. For instance, the data protection provisions under the PDPA do not apply to personal data that has been contained in a record that has been in existence for at least 100 years. In addition, personal data pertaining to deceased individuals is also excluded from most of the obligations under the PDPA. In relation to such data, organisations will be subject only to the requirements to make reasonable security arrangements for the protection of such data, and the requirements relating to disclosure of personal data. These reduced obligations will apply for 10 years from the deceased's date of death. In this regard, an individual appointed under the deceased's will to exercise such rights (or, if there is no such person, the deceased's nearest relative) may exercise all or any of the following rights in relation to the protection of the deceased's personal data:

- the right to give or withdraw any consent for the purposes of the PDPA;
- the right to commence a private civil action in respect of any loss or damage suffered from a contravention of any of the provisions under Parts IV to VI of the PDPA; and
- the right to bring a complaint under the PDPA.

While the PDPA does not distinguish between the treatment of personal data of minors and that of individuals above 21 years of age, the PDPC has, in its Selected Topics Guidelines, recommended that organisations take appropriate steps to ensure that a minor can effectively give consent on his or her own behalf, in light of the circumstances of the particular case including the impact on the minor in giving consent. In this regard, the PDPC has also indicated that it will adopt the practical rule of thumb that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his or her own behalf. However, where, for example, an organisation has reason to believe or it can be shown that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from an individual who is legally able to provide consent on the minor's behalf (eg, his or her parent or other legal guardian).

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The obligation to notify stems primarily from the process of seeking valid consent (see question 11). In particular, organisations are obliged to inform individuals of:

(i) the purposes for the collection, use or disclosure of his or her personal data, on or before collecting the personal data;
(ii) any other purpose for the use or disclosure of personal data that has not been notified to the individual under (i), before such use or disclosure of personal data; and
(iii) on request by the individual, the business contact information of a person who is able to 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 in accordance with the purposes made known to him or her.

While the 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.

In relation to personal data that was collected by an organisation prior to the data protection provisions under the PDPA coming into effect on 2 July 2014, there is no express requirement under the PDPA that requires the organisation to notify individuals whose personal data they hold. However, fresh consent would need to be obtained from the individual concerned where the personal data collected is to be used for a different purpose from that to which consent was originally given. It follows that notification of the new purposes for which the personal data is to be collected, used or disclosed would also be required.

14 Exemption from notification

When is notice not required?

In addition, the Second, Third and Fourth Schedules to the PDPA also 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 (see question 11 for more details). Accordingly, the notification obligation would not apply under such circumstances.

However, section 20(4) of the PDPA carves out an exception to this concession. An organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of managing or terminating an employment relationship, has the obligation to inform the individual of that purpose; and, on request by the individual, the business contact information of a person who is able to answer the individual's questions about the collection, use and disclosure on behalf of the organisation. This is despite the fact that the same organisation has no obligation to seek the consent of the individual before collecting, using or disclosing personal data for such purposes.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

There is no specific requirement under the PDPA that compels organisations that hold the personal data of individuals to offer such individuals the right to have a degree of choice or control over the use of their personal data.

However, individuals have a right under section 16 of the PDPA to withdraw consent (including deemed consent) given to an organisation in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. The individual would need to give reasonable notice to the organisation as to the withdrawal of his or her consent. Thereafter, upon receipt of such notice, the organisation would need to inform the individual of the likely consequences of the withdrawal of consent, although the organisation should not prohibit the individual from withdrawing consent. Where the individual has withdrawn his or her consent, organisations would be required to inform their data intermediaries and agents to similarly cease collecting, using or disclosing the personal data of this individual.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

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 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.

The Key Concepts Guidelines also state that organisations, in deciding what is considered a reasonable effort, should take into account the following factors:

- the nature of the data and its significance to the individual concerned (eg, whether the data relates to an important aspect of the individual such as his or her health);
- the purpose for which the data is collected, used or disclosed;
- the reliability of the data (eg, whether it was obtained from a reliable source or through reliable means);
- the currency of the data (that is, whether the data is recent or was first collected some time ago); and
- the impact on the individual concerned if the personal data is inaccurate or incomplete (eg, based on how the data will be used by the organisation or another organisation to which the first organisation will disclose the data).

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes, section 25 of the PDPA provides that organisations (including data intermediaries) should cease to retain personal data, or remove the means by which 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 in order 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.

In addition, the PDPC in its Key Concepts Guidelines has clarified that personal data should not be kept by an organisation 'just in case' it may be needed. However, personal data may be retained so long as one or more of the purposes for which it was collected remains valid.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes, the purposes for which personal data can be used or disclosed by organisations is restricted to the purposes for which the individual concerned had given his or her consent to the organisation in respect of the same.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

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 (see question 11).

Security

20 Security obligations

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

Section 24 of the PDPA requires that organisations make 'reasonable security arrangements' to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Organisations that process personal data on behalf of an organisation (ie, data intermediaries) are also subject to the same requirement. While the PDPC has recognised that there is no one-size-fits-all solution, it has, in its Key Concepts Guidelines, noted that an organisation should:

- 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.

In this regard, the PDPC has also published the following guidance documents to aid organisations in the management of electronic personal data and data breaches respectively:

- Guide to Securing Personal Data in Electronic Medium (Electronic Data Guide); and
- Guide to Managing Data Breaches (Data Breach Guide).

The Electronic Data Guide sets out good infocommunications technology (ICT) security measures that organisations should adopt to protect electronic personal data (eg, in relation to ICT security audits and tests, authentication and authorisation, computer networks and email security); while the Data Breach Guide provides some guidance for organisations as to the effective management of data breaches.

21 Notification of data breach

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 presently no strict requirement prescribed under the PDPA to notify the PDPC or individuals of breaches of data security. However, in its Public Consultation on Approaches to Managing Personal Data in the Digital Economy, the PDPC has proposed a mandatory data breach notification requirement under the PDPA, to better oversee the level of incidences and management of data breaches at the national level. According to the PDPC's responses to the public consultation (published 8 April 2018), the PDPC has proposed that organisations notify both the affected individuals and the PDPC in situations where the breach is 'likely to result in significant harm or impact to the

individuals to whom the information relates'. In contrast, where the breach does not pose any risk of impact or harm to affected individuals, but is of a significant scale (eg, 500 affected individuals), the PDPC has proposed that organisations notify the PDPC only.

In relation to the time-frame for notification, the PDPC has stated in its response that it intends to provide for an assessment period of up to 30 days from the day the organisation first becomes aware of a suspected data breach, to assess whether the suspected data breach is eligible for notification. Following the organisation's assessment, where the organisation determines that the data breach is eligible for reporting, then the organisation must notify the relevant parties within the required time-frame (ie, 'as soon as practicable' to affected individuals, and 'as soon as practicable, no later than 72 hours' to the PDPC, from the time of determination). At the time of writing, the mandatory data breach notification requirement is not in effect yet, but is expected to be implemented in due course.

In addition to this, the Data Breach Guide states that it is good practice to notify individuals affected by a data breach, and that such notification should be given immediately if sensitive personal data is compromised. This is to allow such individuals to take necessary actions to prevent potential abuse of the compromised data.

Further, the Data Breach Guide recommends that organisations notify the PDPC as soon as possible of any data breach that might cause public concern or where there is a risk of harm to a group of affected individuals. Such notification should include the following information:

- the extent of the data breach;
- the type and volume of personal data involved;
- the cause or suspected cause of the breach;
- whether the breach has been rectified;
- the measures and processes that the organisation had put in place at the time of the breach;
- information on whether affected individuals were notified or when the organisation intends to do so; and
- contact details of persons with whom the PDPC may liaise for further information or clarification.

In this regard, the Data Breach Guide also states that whether organisations notify the PDPC of such data breaches, and whether they have adequate recovery procedures in place, will affect the PDPC's decision on whether an organisation has reasonably protected the personal data under its control or possession.

In addition, one of the mitigating factors that the PDPC may consider when determining a financial penalty to be imposed on an organisation that has breached the PDPA, is whether the organisation voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach and cooperated with the PDPC in its investigations (see question 4).

In addition, where criminal activity (eg, hacking, theft or unauthorised system access by an employee) is suspected, the Data Breach Guide also provides that the police should be notified.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Yes, section 11 of the PDPA specifically requires that organisations designate one or more individuals to be the organisation's data protection officer (DPO). This may be a person whose scope of work solely relates to data protection or a person in the organisation who takes on this role as one of his or her multiple responsibilities. The business contact information of at least one of these DPOs would need to be made known to the public.

The DPO is responsible for ensuring that the organisation complies with the provisions of the PDPA, although the designation of a DPO does not relieve an organisation of its obligations and liabilities (in the event of non-compliance with these obligations) under the PDPA.

The public guidance published on the PDPC's website as of June 2018 sets out that the possible 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 with regard to personal data; and
- liaising with the PDPC on data protection matters, if necessary.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Yes, in order to be able to comply with access requests by individuals (see question 37), the Key Concepts Guidelines state that organisations are generally required to implement processes to keep track of the collection, use and disclosure of all personal data under their control, including unstructured data.

Organisations are also required under section 24 of the PDPA to make reasonable security arrangements to prevent the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to any personal data in their possession or under their control. While the PDPC has recognised that there is no one-size-fits-all solution for organisations, it has, in its Key Concepts Guidelines, noted that an organisation should:

- 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.

Organisations are also expected to cease retaining documents containing personal data, or remove the means by which personal data is associated with particular individuals, as soon as it is reasonable to assume that the purposes for which the personal data was collected is no longer being served by its retention, or the retention of the same is no longer necessary for legal or business purposes.

The obligations above would apply to both the principal organisation and the data intermediary alike.

24 New processing regulations

Are there any obligations in relation to new processing operations?

There is presently no strict requirement prescribed under the PDPA for organisations to apply a privacy-by-design approach or carry out a privacy impact assessment. However, the DPIA Guide states that it is good practice for organisations to conduct regular Data Protection Impact Assessments (DPIAs) to assess and address personal data protection risks specific to the organisation. This would allow organisations to better assess their compliance with the PDPA, and thereafter implement appropriate operational or technical safeguards. The DPIA Guide describes the key aspects of a DPIA.

In brief, organisations should:

- provide an overview of the project and the key considerations surrounding the DPIA;
- define the scope of the DPIA, such as identifying the specific system or process that the DPIA needs to be carried out on;
- define the risk assessment framework or methodology for the DPIA;
- identify the parties whose inputs or views would have to be sought during consultation or interview sessions; and
- provide an estimate of time required for key tasks and overall timeline for conducting the DPIA.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

No, there is presently no such requirement under the 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 PDPC.

However, individuals may register their Singapore telephone numbers on one of the three DNC registers (for faxes, voice calls and text messages, including SMS or MMS messages, and any data applications that use a Singapore telephone number such as WhatsApp, iMessage or Viber). Individuals and organisations intending to make tele-marketing calls or send telemarketing messages (collectively referred to as specified messages) are required to check the relevant DNC registers within 30 days before sending such messages to ensure that recipient tele-phone numbers have not been registered before sending such specified messages.

26 Formalities

What are the formalities for registration?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

With regard to the formalities for registration of Singapore telephone numbers on the DNC registers, as express registration is no longer offered from 23 May 2016, individuals may apply to add or remove their Singapore telephone number to or from the registers by any one of three methods:

- by calling a toll-free number to access the automated Interactive Voice Response System (IVRS), which will provide step-by-step instructions;
- by sending a text message to a designated number; or
- by registering online through the DNC registry website.

The registration of a Singapore telephone number on the DNC registry is free of charge and permanent until withdrawn by the user or subscriber, or until the relevant telecommunications service linked to the number is terminated.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

However, organisations that make telemarketing calls or send specified messages are required to check the DNC registers regularly to ensure that recipient telephone numbers have not been registered on the relevant register, unless they have obtained clear and unambiguous consent in evidential form from the recipients. Failing to do so would be a contravention of the DNC registry rules under the PDPA, and would amount to an offence for which a fine of up to S$10,000 may be imposed.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

As for the DNC registry, only Singapore telephone numbers may be registered. Thus, non-Singapore telephone numbers cannot be registered on any of the DNC registers.

29 Public access

Is the register publicly available? How can it be accessed?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

Organisations that send specified messages are required, within 30 days before sending such messages, to check the DNC registry before sending any such messages.

To access the DNC registry to perform such checks against the DNC registers, organisations are required to apply for an online account through the DNC registry website. This is a one-time application that results in the creation of a main account for the organisation. Main account holders can create as many sub-accounts as required. Creation of an account is open to organisations registered in Singapore, overseas organisations, and individuals (eg, freelancers and agents who conduct telemarketing activities). Fees are payable for creating main and sub-accounts, as well as for running checks on the DNC registry.

An account holder pays one 'credit' (or one to two cents, depending on the pre-paid credit package) for each phone number that is checked. From 1 June 2015, each main account receives 1,000 free credits every year (up from 500 free credits previously), which are valid for one year from the date the free credits are given, as a measure to help organisations, especially small and medium-size enterprises, comply with the DNC provisions by slightly defraying the costs of running such checks on the DNC registry.

30 Effect of registration

Does an entry on the register have any specific legal effect?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

Individuals who register their Singapore telephone numbers on the DNC registry can expect to stop receiving unsolicited telemarketing messages on their registered telephone numbers 30 days after registration.

31 Other transparency duties

Are there any other public transparency duties?

While there is no obligation on an organisation to make public statements on the nature of its processing of personal data per se, section 12 of the PDPA (also known as the Openness Obligation) requires an organisation 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 known to the public.

As part of the Openness Obligation, an organisation is required to appoint a DPO and make available his or her contact details to the public. As good practice, the business contact information of the DPO should be readily accessible from Singapore, operational during Singapore business hours and, in the case of telephone numbers, be Singapore telephone numbers (see question 22).

For completeness, an organisation is also required under section 21 of the PDPA to provide individuals with the following information upon request:

- their personal data that is in the possession or under the control of the organisation; and
- information about the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access (see question 37).

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Organisations that process personal data on behalf of another organisation (the principal organisation) are considered 'data intermediaries' under the PDPA. Such data intermediaries are exempt from most of the main data protection provisions under the PDPA. Data intermediaries are subject only to the data protection provisions relating to the protection and retention of personal data. Specifically, they are required to:

- make reasonable security arrangements to protect personal data in their possession or under their control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
- anonymise or cease retaining personal data, 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.

The principal organisation is subject to the full suite of data protection obligations under the PDPA as if it were processing the personal data itself.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosure of personal data to other recipients must be in accordance with the applicable requirements under the PDPA (see questions 11 and 13).

Furthermore, in certain circumstances the PDPA restricts an organisation from providing an individual with:

- his or her personal data that is in the possession or under the control of the organisation; or
- information about the ways in which his or her personal data has been or may have been used or disclosed by the organisation within a year before the date of the request, in the situation where an individual has requested access to such personal data or information pursuant to the PDPA. See question 37 for a list of circumstances under which an individual's right to access his or her personal data is restricted.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Yes, section 26 of the PDPA prohibits organisations from transferring personal data out of Singapore except in accordance with 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 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.

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.

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; and
- 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, where:

- the individual consents to the transfer of the personal data to that recipient in that country or territory, after being provided with a reasonable summary in writing of the extent to which the personal data to be transferred will be protected to a PDPA-comparable standard, provided:
  - such consent was not required by the transferring organisation as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; and
  - the transferring organisation did not obtain or attempt to obtain such consent by providing false or misleading information about the transfer, or by using other deceptive or misleading practices;
- the transfer of the personal data to the recipient is necessary for the performance of a contract between the individual and the transferring organisation, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organisation;
- 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 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 if a reasonable person would consider the contract to be in the individual's interest;
- the transfer of the personal data to the recipient is necessary for the personal data to be used:
  - for any purpose that is clearly in the interests of the individual (if consent for its use cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent);
  - to respond to an emergency that threatens the life, health or safety of the individual or another individual; or
  - in the national interest;
- the transfer of the personal data to the recipient is necessary for the personal data to be disclosed:
  - for any purpose that is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way;
  - to respond to an emergency that threatens the life, health or safety of the individual or another individual;
  - where there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way (provided that the transferring organisation notifies the individual whose personal data is disclosed of such disclosure and the purposes for such disclosure, as soon as may be reasonably practicable);
  - in the national interest; or
  - for the purpose of contacting the next of kin or a friend of any injured, ill or deceased individual;
- 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 (other than the transferring organisation or an employee of the transferring organisation) while the personal data is in Singapore, except for the purpose of such transportation); or
- the personal data is publicly available in Singapore.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, there is presently no such requirement under the PDPA to notify the PDPC of transfers of personal data.

36 Further transfer

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 imposes an obligation on organisations transferring personal data out of Singapore 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 (see question 34). Where organisations use contractual clauses for the purpose of

imposing such 'legally enforceable obligations', the PDPC, in its Key Concepts Guidelines, distinguishes between data intermediaries and all other organisations (see questions 10 and 32 for more information on data intermediaries).

Where the recipient is a data intermediary, the transferring organisation has to set out minimal protections with regard to 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 with regard to:

- the purpose of collection, use and disclosure by the recipient;
- accuracy;
- protection;
- retention limitation;
- policies on personal data protection;
- access; and
- correction.

The PDPA does not explicitly require transferring organisations to ensure that the 'legally enforceable obligations' imposed on recipients apply to onward transfers of personal data to third-party organisations. However, to the extent that recipients are bound by legally enforceable obligations to provide a PDPA-comparable standard of protection in respect of the transferred personal data, recipients would similarly be obliged to ensure that any onward transfers of personal data are conducted in accordance with the requirements of the PDPA.

Rights of individuals

37 Access

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

Yes, under section 21 of the 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 the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access.

This individual's right of access is subject to a number of exceptions. 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:

- threaten the safety or physical or mental health of an individual other than the individual who made the request;
- cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- reveal personal data about another individual;
- 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
- be contrary to the national interest.

Further, the Fifth Schedule to the PDPA sets out certain situations where organisations are not required to accede to such requests. For example, organisations need not provide access to personal data or information as to how the personal data has been or may have been used or disclosed, in respect of:

- 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 information that is trivial; or
  - that is otherwise frivolous or vexatious.

In addition, an organisation must not inform an individual that it has disclosed his or her personal data without his or her consent pursuant to certain exceptions under the Fourth Schedule to the PDPA, namely where:

- the disclosure is necessary for any investigation or proceedings; or
- the personal data is disclosed to any duly authorised officer of a prescribed law enforcement agency.

Under the PDP Regulations, organisations are entitled to charge the individual a reasonable fee for access to his or her personal data. 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. Under the PDPA, organisations are also 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).

In a situation where two or more individuals make an access request at the same time for their respective personal data captured in the same records, the Key Concepts Guidelines provide that:

- the organisation is required to provide each individual with access only to his or her own data unless consent from the other parties is obtained; and
- the prohibition under section 21(3)(c) of the PDPA does not apply where the other individual has consented to the disclosure of his or her personal data, or where any of the exceptions listed under the Fourth Schedule of the PDPA may apply.

The Key Concepts Guidelines further provide that:

- if an organisation is able to provide an individual with his or her personal data and other information without the personal data or other information excluded under sections 21(2), (3) and (4) of the PDPA, then an organisation must do so; and
- if an organisation has scheduled a periodic disposal of personal data, but has received an access request prior to such disposal, then it should identify such requested personal data as soon as reasonably possible and preserve the personal data while the access request is being processed.

In addition, the Access Requests Guide recommends, among other things, that:

- organisations should clearly make access request channels available (eg, access requests may be submitted in person, through email or by post);
- organisations should keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected, the rationale being that such proper documentation may help organisations in the event of a dispute or an application to the PDPC for a review;
- organisations should implement appropriate retention policies for the keeping of such records (ie, organisations should cease to retain records containing the individual's personal data where retention is no longer necessary for any legal or business purposes); and
- organisations should preserve the personal data requested while processing an access request; for a duration of minimally 30 days after rejecting an access request; and for the whole duration when the PDPC is conducting a review of an organisation's rejection of the access request and until any right of an individual for reconsideration and appeal is exhausted.

38 Other rights

Do individuals have other substantive rights?

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. For instance, organisations need not correct any error or omission in any personal data about the individual that is in the possession or under the control of the organisation, upon request by the individual concerned, if the request relates to:

- opinion data kept solely by the organisation for an evaluative purpose;
- any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
- personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
- personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; or
- a document related to a prosecution if all proceedings related to the prosecution have not been completed.

Unlike access requests, organisations are not entitled to charge a fee for correction requests. Under the PDPA, 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 make the correction). 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.

The PDPA also provides an individual with the right to commence a private action against an organisation where such an individual has suffered loss or damage directly as a result of non-compliance by the organisation of the data protection provisions under Parts IV to VI of the PDPA, subject to certain limitations (see question 39).

39 Compensation

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 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 VI of the PDPA will have a right of action for relief in civil proceedings in a court. However, where the PDPC has made a decision under the PDPA in respect of such a 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.

40 Enforcement

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

The 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. As mentioned, however, such 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 a 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 or correct personal data; or
- pay a financial penalty of up to S$1 million.

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

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The application of the data protection provisions does not extend to 'business contact information', 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 personal purposes'.

In addition, organisations are allowed to continue using (which could include disclosure that is necessarily part of such use) personal data collected before 2 July 2014, for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual indicates or has indicated to the organisation that he or she does not consent to the use or disclosure of the personal data.

In relation to the DNC provisions, the following messages are excluded from the meaning of a specified message under the Eighth Schedule to the PDPA and therefore not subject to the application of the DNC provisions:

- 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 with respect to 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 in relation to a subscription, membership, account, loan or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of goods or services offered by the sender, the sole purpose of which is to provide:
  - notification concerning a change in the terms or features;

Update and trends

PDPC Public Consultation on Approaches to Managing Personal Data in the Digital Economy

There have been rapid developments in Singapore's digital space, with the growth of Internet of Things devices, machine learning and artificial intelligence, as well as developments in the spheres of cloud computing and e-commerce. Data is an integral part of the digital economy, and as society becomes increasingly digitalised, the risk, scale and impact of data breaches will also increase. Cross-border data flows, whether within ASEAN or beyond the region, have also become the norm for a large majority of businesses with a presence in Singapore.

With the fast emergence of the digital economy, the PDPC has taken steps to review the PDPA as part of two public consultations, the Public Consultation for Approaches to Managing Personal Data in the Digital Economy (issued 27 July 2017), and the Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (issued 27 April 2018). While none of the proposed changes has been implemented, it is likely that the data privacy landscape in Singapore will change in tune with the digital economy, and developments in this sphere should be closely monitored.

Extraterritorial applicability of the EU's GDPR

On 25 May 2018, the General Data Protection Regulation (GDPR) came into force and replaced the Data Protection Directive 95/46/EC of the European Parliament and the Council of 24 October 1995. The GDPR applies to organisations that are established in the EU and which process personal data belonging to individuals in the EU, regardless of whether the processing itself takes place within the EU. However, an organisation based outside of the EU (eg, in Singapore) is also subject to the GDPR if it processes personal data belonging to individuals in the EU in the context of:

- offering goods or services to such individuals in the EU (whether or not payment for such goods or services is required); or
- monitoring their behaviour insofar as the behaviour of such individuals takes place within the EU.

The PDPC has published a factsheet to highlight the key requirements of the GDPR to organisations in Singapore, available from the PDPC website.

  - notification of a change in the standing or status of the recipient; or
  - at regular periodic intervals, account balance information or other type of account statement;
- 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.

In addition, the Personal Data Protection (Exemption from Section 43) Order 2013 exempts individuals and organisations sending specified messages to Singapore telephone numbers from the requirement to check the DNC registry, where they have an ongoing business relationship with the subscribers or users of those Singapore telephone numbers. However, the application of the exemption is subject to a number of conditions:

- at the time of the transmission of the specified message, the sender has to be in an ongoing relationship with the recipient;
- the purpose of the specified message has to be related to the subject of the ongoing relationship;
- only specified text and fax messages may be sent to the recipient. Specified messages sent by way of voice calls are not covered by the exemption;
- the specified message has to contain an opt-out facility for recipients to give an opt-out notice to opt out of any exempt message from the sender; and
- the recipient has not withdrawn his or her consent to be sent, or indicated his or her lack of consent to or opted out of being sent, the specified message.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes. However, organisations aggrieved by the PDPC's decision or direction must first:

- request the PDPC to reconsider its decision or direction and thereafter appeal to the Data Protection Appeal Panel; or
- appeal directly to the Data Protection Appeal Panel without submitting a reconsideration request.

Only if such organisation is still aggrieved by the decision of the Data Protection Appeal Panel may it appeal against the Data Protection Appeal Panel's decision to the High Court. An appeal to the High Court can only be made on limited grounds, namely on a point of law or where such decision relates to the amount of a financial penalty.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The 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 PDPA. However, 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 (but are not limited to) 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 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.

In addition, 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.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Organisations that make telemarketing calls or send messages of a commercial nature are required to check the DNC registry at least once every 30 days before sending any such marketing messages, unless they have obtained clear and unambiguous consent from the recipients in evidential form. See question 29 for details on how checks on the DNC registry can be conducted.

Regarding the rules on marketing by email, the Spam Control Act governs the sending of unsolicited emails or spam in Singapore. For more details on the specifics of contravening these rules, see question 6.

As mentioned above, the PDPC is proposing to review, streamline and merge the DNC provisions of the PDPA and the Spam Control Act into a single legislation governing all unsolicited commercial messages, and is currently seeking comments on this as part of its Public Consultation for Managing Unsolicited Commercial Messages and the

Provision of Guidance to Support Innovation in the Digital Economy (see question 1).

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Generally, cloud computing service providers (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. While there is no one-size-fits-all approach in complying with this obligation, the guidance issued by the PDPC may be relevant in assessing whether a CCSP has fulfilled its obligation. For instance, the Data Breach Guide sets out broad steps that organisations may consider taking in planning for and responding to data breaches as well as the Electronic Data Guide, which sets out a good number of practices for organisations to take to protect electronic personal data.

In addition, while the following standards and guidelines are not legally binding per se, these standards and guidelines may also be relevant in assessing whether a CCSP has met the obligation to implement reasonable security arrangements to protect personal data in its possession or under its control under the PDPA:

- Multi-Tier Cloud Security Standard for Singapore 584, a set of security standards issued by the Singapore Information Technology (IT) Standards Committee for voluntary adoption by CCSPs, which provides for three tiers of security certification (tier 1 being the base level and tier 3 being the most stringent); and
- Cloud Outage Incident Response Guidelines (COIR), issued by the Info-communications Development Authority of Singapore (as the IMDA was previously known) on 26 February 2016 for voluntary adoption by CCSPs, guides CCSPs in planning for and responding to cloud outages. The main objective of the COIR is to provide a tiered framework for transparency in cloud service providers' cloud outage incident response for cloud users. Under the COIR, cloud users would be able to opt for the appropriate tier of outage protection and data breaches notification so as to complement their own business continuity and IT disaster recovery capabilities, including fulfilling any legal and regulatory duties.

DREW & NAPIER

Lim Chong Kin **chongkin.lim@drewnapier.com**

10 Collyer Quay
10th Floor, Ocean Financial Centre
049315 Singapore

Tel: +65 6531 4110
Fax: +65 6535 4864
www.drewnapier.com

Spain

Alejandro Padín, Daniel Caccamo, Katiana Otero, Álvaro Blanco, Pilar Vargas, Raquel Gómez and Laura Cantero

J&A Garrigues

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The data protection legislative framework in Spain as of 25 May 2018 is Regulation 2016/679 of the European Parliament and the Council (GDPR), of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

From a local perspective, the Spanish Data Protection Bill is currently in progress before the Parliament and is expected to be approved in the coming months. However, until this new law comes into force, the previous Constitutional Law 15/1999 for the Protection of Personal Data (LOPD) shall apply to those aspects where it does not conflict with the GDPR. Additionally, the Implementing Regulation of the LOPD (Royal Decree 1720/2007) is also applicable.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The state data protection authority is the Spanish Data Protection Agency (SDPA), although there are two authorities with regional powers (especially in the public sector): the Catalonia data protection authority and the Basque data protection authority.

The main powers of the SDPA are:

- carrying out investigations;
- notifying alleged infringements of the GDPR;
- issuing penalties;
- ordering the controller or the processor to comply with the data subject's requests to exercise his or her rights;
- accrediting and issuing certifications;
- authorising contractual clauses, administrative arrangements and binding corporate rules;
- issuing reports on legislation with an impact on data protection; and
- providing information to data subjects.

3 Legal obligations of data protection authority

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

The GDPR provides in article 51 that each supervisory authority shall contribute to the consistent application of the Regulation throughout the EU. For that purpose, the supervisory authorities shall cooperate with each other and the Commission. Accordingly, the GDPR dedicates a chapter to regulate:

- cooperation between supervisory authorities;
- mutual assistance; and
- joint operations.

4 Breaches of data protection

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 several administrative sanctions, according to the type of breach involved. The GDPR establishes a list of different infringements covering two levels of breaches, to which it assigns different administrative fines:

- up to €10,000,000 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; and
- up to €20,000,000 or, in the case of an undertaking, up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

A breach of the data protection law does not involve a criminal penalty, although in some very serious cases the criminal code includes some figures that refer to data protection-related matters.

The SDPA is the administrative body that processes breaches of data protection legislation and the person or entity against whom the complaint is made has various submissions phases. Once the SDPA's decision is made, it may be appealed at the National Appellate Court (continuation of the administrative phase).

Scope

5 Exempt sectors and institutions

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

The GDPR is not applicable to the processing of personal data:

- in the course of an activity which falls outside the scope of EU law;
- maintained by an individual solely in order to carry out purely personal or domestic activities; or
- 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.

In addition to the above, the Spanish Data Protection Bill is not applicable to processing activities:

- subject to legislation on protection of classified materials; or
- regarding deceased persons, with some exceptions.

The Spanish Data Protection Bill also provides that, in connection with the following processing activities, there are a series of matters to which it is applicable where this is expressly stated and which in other scenarios are governed by specific legislation:

- those regulated by legislation on the electoral regime;
- those carried out in the field of penitentiary institutions; and
- those resulting from the Civil Registry or the Central Register of convicted persons and fugitives.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

No. The interception of communications is regulated by Law 13/2015 of 5 October 2015 modifying the Criminal Procedure Law in order to strengthen procedural guarantees and the regulation of technology-related investigation measures.

Commercial communications are in turn regulated in the Information Society Services and Electronic Commerce Law 34/2002 (LSSI).

Finally, in relation to the monitoring and surveillance of individuals, there are no specific laws on the subject, although the SDPA does have guidelines on video surveillance, as well as on labour- and employment-related matters.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

There are numerous laws and regulations that include data protection in their provisions:

- in relation to insurance, Law 26/2006, of 17 July 2006, on insurance mediation and private reinsurance;
- in relation to employment, Law 31/1995, of 8 November 1995, on the prevention of occupational risks;
- in relation to health (especially the regulation of clinical records), Law 41/2002, of 14 November 2002, regulating the autonomy of the patient and the rights and obligations in terms of clinical information and documentation;
- in relation to money laundering, Law 10/2010, of 28 April 2010, on the prevention of money laundering and terrorist financing;
- in relation to telecommunications, the General Telecommunications Act 9/2014, of 9 May 2014; and
- in relation to information society services and electronic commerce, the LSSI.

8 PII formats

What forms of PII are covered by the law?

There are exceptions, such as processing activities carried out:

- in the course of an activity that falls outside the scope of EU law;
- by the member states when carrying out activities that fall within the scope of Chapter 2 of Title V of the Treaty on the European Union (specific provisions on the common foreign and security policy);
- by a natural person in the course of a purely personal or household activity; or
- by competent 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.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

No. The GDPR provides a territorial scope of application broader than Directive 95/46/CE. In addition to the application of the GDPR to controllers and processors established in the EU, the Regulation also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU where the processing activities are related to:

- the offering of goods or services to data subjects in the EU; or
- the monitoring of data subjects' behaviour as far as their behaviour takes place within the EU.

The GDPR also applies to the processing of personal data by a controller established in a place where member state law applies by virtue of public international law.

10 Covered uses of PII

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

The GDPR is applicable to all types of personal data processing, without prejudice to the exceptions mentioned below. However, the GDPR provides the following distinction:

- a 'controller' determines the purposes and means of the processing of personal data; and
- a 'processor' acts and processes data on behalf of the controller.

Following the principle of 'accountability' under the GDPR, the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to the processing of personal data set forth in the GDPR and the lawfulness of such processing. Additionally, the controller shall, among others, answer data subjects' requests to exercise their rights, provide them with the information on processing required under the GDPR, notify personal data breaches and carry out data protection impact assessments.

In contrast, the processor acts on the controller's behalf. Therefore, the processor may perform any of the aforementioned duties, but should carry them out following the instructions provided by the controller. Nevertheless, if a processor infringes the GDPR and processes data for its own purposes and determines the means of the processing, it shall be considered to be a controller with respect to such processing.

The GDPR expressly establishes that the controller and the processor must sign a data processing agreement including the obligations of the processor, which are, among others, to:

- process data following the instructions given by the controller;
- fulfil the duty of confidentiality;
- implement the security measures determined by the controller;
- engage a sub-processor only if authorised by the controller;
- assist the controller in responses to the data subjects' exercise of rights;
- collaborate in the fulfilment of the obligations of the controller; and
- delete or return all personal data processed once the processing ends.

In addition, there are obligations that shall be fulfilled by both the controller and the processor, such as cooperating with the supervisory authority.

Legitimate processing of PII

11 Legitimate processing – grounds

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

Article 6 of the GDPR states the legal bases for the processing of personal data, which are:

- the data subject's consent, which must be unequivocal and given by a clear affirmative act;
- the performance of a contract to which the data subject is party or in order to to take steps prior to engaging into a contract;
- compliance with a legal obligation to which the controller is subject;
- for the purposes of protecting the vital interests of the data subjects or of another natural person;
- the performance of a task carried out in the public interest or in the exercise of official authority; and
- the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subjects.

The SDPA has issued a guideline providing that each processing activity and purpose must be linked to one legal basis. Therefore, whenever there are several purposes for the processing, each purpose may only be based on one legal ground.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Indeed, the GDPR provides that the processing of personal 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 shall be prohibited. However, such personal data may be processed if one of the exceptions provided in article 9.2 of the GDPR applies, among which are:

- explicit consent;
- the processing is necessary for 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 data subjects' vital interests; or
- processing is necessary for reasons of substantial public interest.

Personal data regarding the commission of criminal or administrative offences may only be processed under the control of an official authority or when the processing is authorised by law.

Notwithstanding the above, the Spanish Data Protection Bill provides that obtaining the data subject's consent is not enough to lift the prohibition on the processing of data for the main purpose of identifying the data subjects' ideology, trade union membership, religion, sexual orientation or racial or ethnic origin.

Additionally, the Bill provides that a law may authorise the processing of data in the field of health when so required by the management of public and private health and social care systems and services or by the execution of an insurance contract to which the data subject is party.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Article 13 of the GDPR imposes the obligation upon data controllers to inform data subjects, before carrying out the processing of their personal data, of:

- the identity and contact details of the controller and the DPO, where applicable;
- the purposes of the processing and the legal basis;
- the recipients of the information; and
- the intention to carry out international transfers of data and the existence or absence of an adequacy decision, where applicable.

Additionally, the following further information shall be provided:

- the period for which the personal data will be stored;
- the existence of rights of the data subjects;
- the right to lodge a complaint with the supervisory authority; and
- the existence of automated decision-making, including profiling.

The SDPA has issued a guideline stating that information shall be provided in a double-layer format. According to this guideline, a first layer with basic information on the processing of data must be included somewhere in the data subject's field of vision. In this context, basic information is considered to include the identity of the data controller, the purpose of the processing activity, the legal basis of said processing activity, any data communication or data transfer that may take place and the rights of the data subject. The second layer shall contain the complete and detailed information mentioned in article 13. Accordingly, the first layer must include links to the different sections of the second layer, so that the data subject can access information easily. The SDPA recommends providing the basic first layer information in table form.

When the data has not been obtained from the data subject, the GDPR imposes in article 14 the obligation to provide information on, in addition to that set forth in article 13, the categories of personal data concerned, and from which source the personal data originates and, if applicable, whether it came from publicly accessible sources. Such information shall be provided within a reasonable period and before it is disclosed to any third party.

14 Exemption from notification

When is notice not required?

The information obligation imposed by articles 13 and 14 of the GDPR shall not be applicable where and insofar as:

- the data subject already has the information;
- providing information to the data subject is deemed impossible or requires a disproportionate effort;
- the collection or disclosure of data is expressly laid down by law; or
- the personal data must remain confidential subject to an obligation of professional secrecy regulated by law.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Data subjects shall always have the possibility of exercising the rights of access (to request and obtain free of charge information on their personal data), rectification (to modify, update and complete their personal data), erasure (to request the blocking of the personal data during the statute of limitations of any liabilities that may arise as a consequence of the processing, making them available only to public administrations, courts and judges and subsequently proceeding to its deletion when such personal data is deemed inadequate or excessive) and, if applicable, opposition (to oppose the processing of personal data or request its ceasing through a free-of-charge procedure), restriction (to oppose the processing of personal data for one or more purposes) and, only when the legal basis applicable is consent or contract, portability (to receive the personal data concerning him or her, which he or she has provided to the controller in a structured, commonly used and machine-readable format or transmit them to another controller).

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Article 5 of the GDPR states that personal data should only be collected for processing when such data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Additionally, personal data should be accurate and updated in order to show adequacy to the actual situation.

Inaccurate or incomplete personal data shall be erased or substituted by the data controller for updated and accurate data. However, the Spanish Data Protection Bill provides that the inaccuracy of the personal data shall not be attributable to the controller, when the controller has taken all reasonable steps to ensure that the data is erased or rectified without delay.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Article 5 of the GDPR, as stated above, indicates that personal data may only be collected and processed if it is adequate, relevant and limited to what is necessary in relation to the purposes of the processing (data minimisation principle). This restricts the amount of data that can be collected.

Regarding the duration of the processing, this same article 5 states that personal data should be 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 (storage limitation principle). Notwithstanding the foregoing, according to the Spanish Data Protection Bill, it may be foreseeable that once this period is covered, personal data should only be kept blocked in order to impede its processing except when public administrations, judges or courts need to access it for the attention of the potential responsibilities raised by the processing, except for limited cases, such as data collected for video-surveillance purposes.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Article 5 of the GDPR states that personal data cannot be processed in a manner that is incompatible with the purposes for which such personal data was collected (purpose limitation principle).

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The exceptions to the finality principle under the GDPR are the further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Security

20 Security obligations

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

The GDPR requires PII controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, 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 risk of varying likelihood and severity for the rights and freedoms of natural persons.

Among others, the GDPR includes a specific reference to the following security measures:

- 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 in a timely manner 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.

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, particularly from accidental or unlawful destruction, loss, alteration and unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

21 Notification of data breach

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 GDPR establishes that, in case of a personal data breach, the PII controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority (in Spain, the SDPA), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Likewise, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the PII controller shall additionally communicate the personal data breach to the data subject without undue delay.

The GDPR determines the minimum content of such communications in terms of the minimum information to be provided to the supervisory authorities and to the affected data subjects.

Additionally, telecommunications legislation includes a notification obligation vested on operators exploiting electronic communications public networks. This legislation indicates that the kind of data breach that implies the notification obligation shall be that which causes the accidental or illicit destruction, loss, alteration, revelation or non-authorised access to personal data transmitted, stored or in any other way processed in relation with an electronic communication service of public access.

In case of a data breach, the operator is obliged to report it to the SDPA without undue delay, describing at least the nature of the breach, its consequences and the proposed and implemented measures respecting the specific breach. If the breach could negatively affect the privacy or personal data of the individual, the operator shall also notify the affected individual, stating the nature of the breach, a contact point where the individual can ask for further clarifications and a series of recommendations regarding the security of the individual's data directed to mitigate the effect of the data breach. The notification to the individual shall not be necessary in cases where the operator has properly explained to the SDPA the breach and the measures implemented to mitigate its effect, and the SDPA has expressly freed the operator from the need to notify the individuals affected.

Operators are also obliged to report to an individual when there is a specific risk of data breach on a public network or electronic communications service. In these cases, the operator shall inform the individual affected of the particular risk and the measures it plans to implement to mitigate the risk.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

According to the GDPR, the appointment of a data protection officer is mandatory:

- when the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- when 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
- when the core activities of the controller or the processor consist of processing on a large scale special categories of personal data pursuant to article 9 of the GDPR and personal data relating to criminal convictions and offences referred to in article 10 of the GDPR.

The main responsibilities of a data protection officer are to:

- inform and advise the controller or processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other EU or member state data protection provisions;
- 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;
- provide advice where requested as regards the data protection impact assessment and monitor its performance;
- cooperate with the supervisory authority;
- act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in article 36 of the GDPR, and to consult, where appropriate, with regard to any other matter.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Data controllers shall maintain a record of processing activities under their responsibility. That record shall contain the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purpose of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or international organisations;

- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of international data transfers, the corresponding suitable safeguards, if applicable;
- where possible, the envisaged time limits for erasure of the different categories of data; and
- where possible, a general description of the technical and organisational security measures applied.

Data processors shall also maintain a record of all categories of processing activities carried out on behalf of a controller.

These obligations 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 data subjects, the processing is not occasional or the processing includes special categories of data as referred to in article 9(1) of the GDPR or personal data relating to criminal convictions and offences referred to in article 10 of the GDPR.

Additionally, SDPA rules establish an obligation consisting of blocking personal data once cancelled. When personal data is no longer necessary for the purposes for which it was collected, it must be cancelled. This cancellation would not imply the automatic suppression of the data, but its blockage.

This blockage consists of the identification and preservation of the personal data by the PII owner in order to impede its processing save when public administrations, judges or tribunals need to access it for the attention of the potential responsibilities raised by the processing. This is an obligation to keep the data on its premises or servers without processing it, only at the disposal of the public authorities mentioned and only during the statute of limitations of the actions that could be derived from the processing of each specific personal data category. Once this period is over, the personal data must be suppressed.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Yes, under the GDPR PII owners are obliged to implement new processing operations, such as privacy-by-design and privacy-by-default approaches, as well as carrying our privacy impact assessments in accordance with the accountability principle.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

No, the GDPR does not foresee the obligation of registry before any supervisory authority. The only registry obligation refers to the appointment of the data protection officer (if required), whose contact details have to be notified to the SDPA.

26 Formalities

What are the formalities for registration?

As mentioned in the previous question, there is no obligation to register files before the supervisory authority.

In order to notify the appointment of a DPO before the SDPA, the controller or processor must fill in a form with the details of the DPO and information on his or her appointment and send it to the SDPA. This notification is free and may be conducted telematically through electronic means.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There are currently no penalties for failure to make or maintain an entry on the SDPA's register, provided that it is no longer an obligation.

Regarding the notification of the appointment of the DPO, we have no information on whether there will be any penalties in case of failure to notify such information.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

As there is no obligation to register data filings with the SDPA, the SDPA no longer provides the possibility to carry out any registrations.

29 Public access

Is the register publicly available? How can it be accessed?

The registered data filings have not been publicly available since 25 May 2018. A copy of the information in the files that were registered with the SDPA before 25 May 2018 may be requested, but such access is restricted to the controller or its representatives, as certain information concerning the data controller must be provided when submitting the request.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Since 25 May 2018, filing entries on the register have no legal effect.

Regarding the DPO's appointment, notification is necessary for compliance with the GDPR, which provides that data controllers and data processors must notify said contact details to the supervisory authority.

31 Other transparency duties

Are there any other public transparency duties?

The GDPR has established an obligation to maintain a record of processing activities for controllers and processors that:

- employ 250 or more employees;
- carry out processing of personal data that is likely to result in a risk to the rights and freedoms of data subjects;
- carry out processing of personal data that is not occasional; or
- carry out processing of personal data that includes special categories of data.

Such record of processing activities must be available to the supervisory authority upon request.

Additionally, the SDPA has issued guidelines for data controllers that provide that, in order to reach transparency, information provided to data subjects must be concise, transparent, intelligible and easily accessible, in clear and simple language. Therefore, the information clauses must be explained in a clear and accessible way for the data subjects and shall be provided in a double-layer format. The GDPR also establishes a more exhaustive list of information to be provided to data subjects, which adds, among others, the legal basis for the processing, the intention to carry out profiling and the contact details of the DPO.

Finally, in the case of a personal data breach, the controller shall, no later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. 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 data subject. Additionally, the controller shall document every personal data breach.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The regime on the disclosure of PII to third parties to provide outsourced processing services to a data processor implies that the PII owner and the data processor shall execute a written agreement regulating the PII flow and the obligations of the data processing (as provided in article 28 of the GDPR). A number of specific references need to be specified, such as the nature of the processing, its duration, its purpose, the categories of personal data and the specific processing activities. Additionally, the GDPR provides obligations for the processor that must be included in the data processing agreement, which include, among others:

- the instructions that the processor must follow;
- the duty of confidentiality;

- the exact description of the security measures that the data processor shall implement for the processing of the data or a reference to the document in which such measures are described;
- the sub-processing regime;
- how the processor will assist the controller in responses to data subjects' exercise of rights;
- collaboration in the fulfilment of the obligations of the controller; and
- the destination of data once the processing ends.

Data processing agreements that were signed before 25 May 2018 must be amended and adapted in order to meet these requirements.

The GDPR also provides that this communication of data may be regulated, in limited cases, by a unilateral act of the controller that defines the position and obligations of the controller.

Additionally, the GDPR and the guidelines issued by the SDPA provide that the controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures so that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Accordingly, processors can adhere to codes of conduct or certify within the framework of certification schemes to prove that they offer such guarantees.

Regarding communication of data to entities located outside the European Economic Area (EEA), see question 34.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

There are no specific restrictions under the GDPR on the disclosure of personal data to other recipients, excepting those general requirements such as the need to respect the general principles of the data protection law and to provide the data subject with the information specified in articles 13 and 14 of the GDPR.

In this connection, the specific information shall be provided to the data subject at the time when the personal data is obtained or, where the personal data has not been obtained from the data subject, within a reasonable period after obtaining the personal data, but at the latest within one month; or, if the personal data is to be used for communication with the data subject, at the latest at the time of the first communication with that data subject. Moreover, if a disclosure to another recipient is envisaged, the referred communication shall be provided to the data subject at the latest when the personal data is first disclosed.

In particular, PII owners shall provide the data subject with the purposes of the disclosure for which the personal data is intended and the legal basis for the disclosure to be made, as well as letting the data subject know the recipients or categories of recipients of the personal data, among other information. In addition, the data subject has the right to obtain from PII owners access to the information regarding the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Transfers of personal data outside the EEA are restricted, bearing in mind that cross-border transfers outside the EEA are not allowed unless the specific legal requirements of articles 44 to 50 of the GDPR are fulfilled. In all cases, PII owners, processors or exporters shall comply with certain specific obligations in order to conduct cross-border transfers.

As a general rule, any transfer of personal data shall take place only when the transfer is to be made to a third country or an international organisation that has been declared by the European Commission as having an adequate level of protection or when the PII owner or processor has provided 'appropriate safeguards', and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

In order to provide 'appropriate safeguards', under the GDPR it is sufficient to apply one of the following safeguards:

- legally binding and enforceable instruments between public authorities or bodies;
- binding corporate rules;
- standard data protection clauses adopted by the European Commission;
- standard data protection clauses adopted by a supervisory authority and approved by the European Commission;
- an approved code of conduct, together with binding and enforceable commitments of the PII owner or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism together with binding and enforceable commitments of the PII owner or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In addition to the foregoing, the GDPR allows transfers of PII outside the EEA when the appropriate safeguards are provided by contractual clauses between the PII owner or processor and the PII owner, processor or the recipient of the PII in the third country or international organisation, or by provisions to be inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subjects' rights.

Notwithstanding the above, article 49 of the GDPR allows transfers of PII outside the EEA for specific situations such as when the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards, or when the transfer is necessary for the performance of a contract between the data subject and the PII owner or the implementation of pre-contractual measures taken at the data subject's request, among other regulated situations.

Finally, for information purposes the PII owner shall let the data subject know if it intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission or, where applicable, make reference to the appropriate or suitable safeguards and the means of obtaining a copy of them or where they have been made available.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, under the GDPR international transfers of PII no longer require the prior notification to or authorisation of the director of the SDPA. As a general rule, transfers of personal data to a third country or an international organisation may take place without any specific authorisation where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question, ensures an adequate level of protection. In the absence of a European Commission decision of adequacy, PII owners or processors may transfer personal data internationally only if the PII owners or processors provide 'appropriate safeguards' (which can be provided, among others, if the parties have executed a bilateral agreement following the standard data protection clauses adopted by a supervisory authority and approved by the European Commission or binding corporate rules have been approved).

Furthermore, PII owners or processors may perform international transfers of personal data by adopting contractual clauses between the PII owner or processor and the PII owner, processor or the recipient of the PII in the third country or international organisation and by provisions to be inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subjects' rights. However, the aforementioned two ways to provide 'appropriate safeguards' shall be subjected to authorisation from the SDPA, as the competent Spanish supervisory authority.

While under the GDPR international transfers of personal data no longer require the prior authorisation of the director of the SDPA, authorisations made under the LOPD shall remain valid until amended, replaced or repealed, if necessary, by the SDPA, as well as decisions of adequacy adopted by the European Commission.

Update and trends

The new data protection act implementing the GDPR is expected to be published in 2018, so a close look at the legislative process has to be kept. Also, a close follow-up of the SDPA and the European Data Protection Committed guidelines is a must for the correct implementation of the GDPR. The project of the new ePrivacy Regulation being negotiated at EU level is also attracting the attention of stakeholders.

36 Further transfer

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

Yes, under the GDPR restrictions to international transfers of personal data equally apply to transfers to be made to service providers (data processors) if these are located in a state that does not provide an adequate level of data protection. Onward transfers from importing PII owners are generally subject to the laws applying in the jurisdiction where the data exporter is located and, therefore, it shall be reviewed whether under such rules any cross-border restrictions or authorisations apply.

Rights of individuals

37 Access

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

Individuals have the right to obtain from PII owners confirmation as to whether or not personal data concerning the data subject is being processed and, where that is the case, access to the personal data and specific information (such as the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipient to whom the personal data has been or will be disclosed, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period, among other information) by addressing a simple petition to the PII owner.

Under the GDPR, individuals not only have the right to access personal data, but also the right to be provided with a copy of the personal data undergoing processing by the PII owner.

The petition has to be responded to without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. If the PII owner does not take action on the request of the data subject, the PII owner shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

The petition has to be responded to free of charge excepting those cases where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character.

38 Other rights

Do individuals have other substantive rights?

Yes, in addition to the right of access, individuals are entitled to the right of rectification, ie, the right to obtain from the PII owner the rectification of inaccurate personal data concerning him or her, as well as the right to have incomplete personal data completed, including by means of providing a supplementary statement; and the right to restrict processing, ie, the right to obtain from the PII owner restriction of processing in specific situations (such as when the accuracy of the personal data is contested by the data subject, for a period enabling the PII owner to verify the accuracy of the personal data or when the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead, among others).

Moreover, individuals have the right to object to the processing of personal data concerning him or her when the processing is based on:

- the performance of a task carried out in the public interest or in the exercise of official authority vested in the PII owner; or
- the legitimate interests pursued by the PII owner or by a third party.

When the data subject objects in either of those cases, the data controller shall no longer process the data, except when the data controller demonstrates compelling legitimate grounds that override the interests or fundamental rights and freedoms of the data subject or if the data is needed for legal claims.

Individuals are also entitled to the right to data portability, ie, the right to receive the personal data concerning him or her that he or she has provided to a PII owner, in a structured, commonly used and machine-readable format, and the right to transmit that data to another PII owner without hindrance from the PII owner to whom the personal data has been provided. In this sense, individuals may exercise the referred right provided that the processing is based on consent or is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract, and the processing is carried out by automated means.

In addition to the above, the GDPR has recognised the right to erasure ('right to be forgotten'), as a particular way to exercise the right to object to the processing of personal data in the online environment. In this connection, the data subject shall have the right to obtain from the PII owner the erasure of personal data concerning him or her provided that one of the specific situations of article 17(1) of the GDPR are fulfilled, such as when the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed or where there is no other legal ground for the processing, among other regulated situations.

39 Compensation

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 claim damages before the courts under general civil legislation if they prove that an infringement to data protection legislation has produced an injury to their assets or feelings. When the data subject claims before the SDPA, the authority shall impose a fine on the PII owner or data processor, but it will not give compensation to the affected individual. The only way to claim those damages is through a civil claim before the ordinary courts. The claim must be based on the evidence of the infringement, the proof of the damages produced on the assets or moral of the individual and the proof of the link between such infringement and those damages.

40 Enforcement

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

Both. The infringement of the data protection law can be reported to the supervisory authority but it can also serve as a basis for an action before the courts. Additionally, there are infringements that may be enforced by the supervisory authority and appealed before the courts.

There are also some especially serious infringements that can be considered criminal offences and give rise to criminal punishments after a trial before the criminal courts.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

In addition to the exclusions set forth in question 5 above, the GDPR does not apply to issues of the protection of fundamental rights and freedoms or the free flow of personal data related to activities that fall outside the scope of EU law, such as activities concerning national security. Neither does it apply to the processing of personal data by the member states when carrying out activities in relation to the common foreign and security policy of the EU.

Additionally, member state law may lay down specific provisions on data protection in order to adapt the application of the rules of the GDPR for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority. As an example, while the GDPR applies to the activities of courts and other judicial authorities, EU or member state law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, PII owners can appeal before the administrative courts, in particular at the Central National Tribunal for administrative cases, which is the only court that can be accessed for this type of appeal. The rulings of this tribunal can be further appealed in exceptional cases before the Supreme Court.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The use of cookies is regulated under the Spanish Information Society Services and Electronic Commerce Act, which transposes the European ePrivacy Directive. Any company using cookies has to inform users at the first access to the website of the use of cookies, offering the user the possibility of accepting or rejecting the cookies. It is accepted that the mere action of the user continuing with the browsing session is deemed as an acceptance of the use of the cookies. The information has to be offered in two layers, the first one being a banner or simple notice in a visible way with simple information about the existence of the cookies, and a second underlying layer (accessible through a link) with complete information on the type of cookies used, their purpose and how to deactivate them.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Electronic communication marketing can only be carried out with the explicit consent of the user. In cases in which the company has an existing contract with a customer, marketing communications can be sent if they refer to the same type of services or products that are the object of the existing contract, but only if this has been informed at the moment of collection of the data, and the possibility of opting out of such reception of marketing communications is given to the individual both at the moment of giving the information and then with each and every communication that is sent.

Telephone marketing is subject to the general rules of data protection (GDPR) and the provisions under consumer protection legislation and competition rules. The main rule is that no automated or persistent communications can be made without the user's consent, and in each communication the user has to be offered the possibility of opting out of receiving other calls.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Cloud computing services are regulated in the same manner as any other provision of services, the provider being considered a data processor when personal data is involved. The only important matter to bear in mind is that the PII owner needs to understand where the personal data is going to be located when using a cloud provider, because it may happen that the servers are located outside the EEA, and then additional formalities regarding international transfers of data might have to be applied, as explained in question 32.

GARRIGUES

Alejandro Padín **alejandro.padin@garrigues.com**

C/ Hermosilla, 3
28001 Madrid
Spain

Tel: +34 91 514 52 00
www.garrigues.com

Sweden

Henrik Nilsson

Wesslau Söderqvist Advokatbyrå

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The primary constitutional law, the Instrument of Government (1974:152), contains a guarantee that everyone shall be protected in their relations with government institutions against significant invasions of their personal privacy, if these occur without their consent and involve the surveillance or systematic monitoring of the individual's personal circumstances.

The central legislation for the protection of PII since 25 May 2018 is the Regulation (EU) 2016/679 (General Data Protection Regulation or GDPR) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. On the same date, the Act (2018:218) with supplementary provisions to the EU Data Protection Regulation (the Data Protection Act), supplemented by an Ordinance (2018:219) (Data Protection Ordinance), came into force.

The Data Protection Act (DPA) authorises the government and such public authority the government designates (primarily the Swedish Data Inspection Board (DIB) but other relevant authorities are also sometimes designated) to issue more detailed regulations concerning several important features of the DPA. This authorisation has been relied on to issue the Data Protection Ordinance (2018:219) and is expected to lead to several Regulations published in the Data Inspection Board Statute Book (DIFS).

EU and Swedish law uses the term 'personal data'. Personal data is defined by the GDPR as 'any information relating to an identified or identifiable natural person'. This chapter will use the term personal data rather than PII.

A great many further acts and ordinances contain regulations regarding personal data registries and other processing of personal data. This body of law is known as the Registry Acts. The Registry Acts cover areas such as law enforcement, financial activities, healthcare and much more. There is no authoritative list of the Registry Acts. Relevant legislation outside of the Registry Acts includes the Camera Surveillance Act (2018:1200) and the Electronic Communications Act (2003:389), implementing the ePrivacy Directive 2002/58/EC.

The text of the European Convention on Human Rights has been incorporated into law in the ECHR Act (1994:1219).

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The supervisory authority regarding data protection is the Swedish Data Inspection Board (DIB), www.datainspektionen.se. The mission of the DIB is, according to the Ordinance (2007:975) instructing the DIB, 'to work to ensure that fundamental human rights are protected in connection with the processing of personal data, to facilitate the free flow of personal data within the European Union and to ensure that good practices are observed in credit and debt collection operations'.

The DIB is a public authority reporting to the Ministry of Justice. It has long been a comparatively small organisation, comprising 55 employees in 2016 (48 full-time positions) with an operating budget for 2016 of approximately 49.8 million kronor. In connection with the introduction of the GDPR, the DIB budget has been given a one-time boost to 85 million kronor for 2018. The DIB is also the supervisory authority for the Debt Recovery Act of 1974 (1974:182), the Credit Information Act of 1973 (1973:1173) and the Camera Surveillance Act of 2018 (2018:1200).

The DIB's Annual Report for 2017 relates that the DIB initiated 21 new ongoing inspection matters during 2017. This is about one-third of the number it initiated in 2016, and reflects the authority's focus on preparing its organisation for the GDPR. The government has floated the idea of changing the name of the DIB to the Authority for the Protection of Privacy (*Integritetsskyddsmyndigheten*). DIB has in response suggested Data Protection Authority (*Dataskyddsmyndigheten*) as a new name. The name issue has at the time of writing (June 2018) not been settled.

The DIB has the power to request access to such personal data that is being processed by someone in its jurisdiction, including access to the premises of the processing. It may request information and documentation regarding the processing and regarding such security measures applied to the processing. The DIB may order that certain security measures shall be applied to the processing, and may prohibit a controller from processing personal data in any other manner than by storing it.

3 Legal obligations of data protection authority

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

Chapter VII of the GDPR regulates cooperation and consistency between EU data protection authorities. Section 1 of Chapter 7 (articles 60 to 62) regulates cooperation, whereas section 2 of the Chapter (articles 63 to 67) establishes a consistency mechanism. The Swedish national supplementary legislation to the GDPR, the Data Protection Act, does not further regulate cooperation and consistency mechanisms.

4 Breaches of data protection

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

Chapter 8 of the GDPR regulates remedies, liability and penalties with regard to data protection. Article 58 of the GDPR grants many varied powers to the data protection authority. The DPA explicitly authorises the DIB to exercise the powers set out in article 58.1–58.3. The DIB is restricted under the DPA to imposing administrative sanctions to the breaches of the GDPR as listed in article 83, and also breaches of article 10. The DIB is authorised to decide administrative sanctions against public authorities should one come to breach the GDPR. The penalty fee for a public authority shall be determined up to a maximum of 5,000,000 kronor in the case of infringements referred to in article 83(4) of the EU Data Protection Regulation, and up to a maximum of 10,000,000 kronor in the case of infringements referred to in article

83.5 and 83.6 of the Regulation. Breaches of the GDPR or the DPA cannot lead to criminal penalties in Sweden, with the exception of a breach of secrecy or confidentiality of a data protection officer concerning the performance of his or her tasks.

Decisions regarding orders or sanctions can, in accordance with DIB internal procedural rules, be taken by the case officer in charge, the head of department or by the director-general, depending on the gravity or importance of the decision. There is no requirement to submit a draft decision to the receiving party for comment prior to adopting it, but this has been known to have happened in a small number of cases.

Scope

5 Exempt sectors and institutions

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

The GDPR and the DPA covers all sectors and types of organisations, public authorities as well as private organisations. If another law or ordinance contains provisions that deviate from the DPA, these provisions have precedence. The Police Data Act of 2010 and the Healthcare Patient Data Act of 2008 are examples of such sector-specific data protection regulation whose provisions interact with the DPA.

The DPA does not apply to such processing of personal data that a natural person performs in the course of activities of a purely private nature.

Article 85 of the GDPR, covering 'Processing and freedom of expression and information', exempts processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression from many provisions of the Regulation. Under Swedish law, an organisation is able for a nominal fee to acquire a 'publishers' certificate' (*utgivningsbevis*), which accords it the status of a media organisation exempted from most GDPR requirements. Such certificates have been acquired by many leading directory services (not to mention other companies operating far from a typical media company) seeking the statutory exemption. It remains to be seen if the present publisher certificate award procedure will withstand future EU scrutiny.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Electronic Communications Act (2003:389) implements ePrivacy Directive 2002/58/EC and Data Retention Directive 2006/24/EC. Some provisions of the ePrivacy Directive are implemented in the Marketing Act (2008:486), such as regarding the use of unsolicited advertising through email.

The Camera Surveillance Act 2018:1200 regulates the use of equipment for audio-visual monitoring and surveillance.

The Act on Interception of Signals for Military Intelligence (2008:717) regulates the interception of cable and radio signals for the purpose of military intelligence.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Laws and regulations providing specific data protection rules related to public authorities number in the hundreds. The DIB supervises the Credit Reporting Act (1973:1173) and the Debt Recovery Act (1974:182). It also has duties under the Healthcare Patient Data Act (2008:355).

Regarding law enforcement, the Police Data Act (2010:361) and the Criminal Records Act (1998:620) may be noted.

Two separate proposals for legislation on privacy in the workplace have been presented in government-commissioned reports since 2002, but have not, to date, led to legislation.

8 PII formats

What forms of PII are covered by the law?

The DPA applies to such processing of personal data as is wholly or partly automated. The DPA may thus be applied to PII in digital video format.

The DPA also applies to other processing of personal data, even in paper format, if the data is included in or is intended to form part of a structured collection of personal data that is available for searching or compilation according to specific criteria, such as an indexed collection of paper documents.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The DPA applies to those controllers of personal data that are established in Sweden.

The DPA also applies to the processing of personal data performed by controllers or processors established only in countries outside the EU/EEA if the processing concerns data subjects located in Sweden and are related to the offering of goods or services to such data subjects, or monitoring their behaviour in Sweden.

10 Covered uses of PII

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

Processing is defined in article 4.2 of the GDPR as any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Article 85 of the GDPR, covering 'Processing and freedom of expression and information', exempts processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression from many provisions of the Regulation.

The GDPR distinguishes between controllers and processors as well as third parties, those natural or legal persons, public authorities, agencies or bodies other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data. Chapter IV, section 1 (articles 24 to 31) of the GDPR sets out the differences of duties of these three categories. Swedish law has not set out any deviations from the GDPR in this regard.

Legitimate processing of PII

11 Legitimate processing – grounds

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

Under the GDPR, personal data may be processed only if a legal basis set out in article 6 applies.

The DPA specifies that the GDPR does not apply if it contravenes the constitutional Freedom of the Press Act and the Fundamental Law on Freedom of Expression.

Personal data may be processed on the basis of article 6(1)(c) or (e) of the GDPR if the processing is necessary for the personal data controller to comply with a legal obligation arising from a law or other regulation, collective labour market agreement or decisions issued under a law or other regulation, or as part of the data protection officer's exercise of authority by a law or other constitution.

Personal data may also be processed on the basis of article 6(1)(e) of the GDPR if the processing is necessary to perform a task of public interest arising from a law or other regulation, collective agreement or decisions issued pursuant to law or other constitution, or as part of the personal data officer's exercise of authority by a law or other regulation.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The GDPR makes a distinction for processing of special categories of personal data, labelled sensitive data under the DPA .

Special categories of personal data are 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.

Sensitive personal data in the field of employment and social security and social protection law may be processed pursuant to article 9(2)(b) of the GDPR if the processing is necessary for the data controller or the registrant to fulfil his or her obligations and exercise his or her special rights in the field of labour law and in social security and social protection.

Personal data thus processed may be disclosed to third parties only if there is an obligation for the data controller to do so or, in the field of social security and social protection, whether the data subject has explicitly agreed to the disclosure.

Processing by a public authority of sensitive personal data that is necessary for reasons of substantial public interest is permitted if the information has been submitted to the authority and the processing is required by law, where the processing is necessary for the handling of a case, or otherwise, if processing is necessary in view of an important public interest and does not constitute an improper infringement of the personal privacy of the data subject.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Under article 13 of the GDPR, if data about a person is collected from the person him or herself, the controller shall, in conjunction with collection, voluntarily provide the data subject with information about the processing of the data.

Under article 14 of the GDPR, if personal data has been collected from a source other than the data subject, the controller shall within a reasonable period after obtaining the personal data, but at the latest within one month, provide the data subject with information about the processing of the data upon registration.

14 Exemption from notification

When is notice not required?

Notification is not required when the data subject already has the information; the provision of such information 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, or insofar as the obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Notification is further exempted where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or member state law, including a statutory obligation of secrecy.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Chapter III (articles 12 to 23) of the GDPR set out extensive data subject rights. These rights have not been restricted or extended further under Swedish law.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Article 5.1(d) of the GDPR imposes standards in relation to the quality, currency and accuracy of personal data. These standards have not been restricted or extended further under Swedish law.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Article 5.1(e) of the GDPR sets out that personal data may be 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. Personal data may be kept for historical, statistical or scientific purposes for a longer time than necessary for the purpose for which it was collected. However, in such cases personal data may not be kept for a longer period than is necessary for these purposes.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Article 5.1 of the GDPR maintains the finality principle. There is no deviating regulation in Swedish law.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Personal data may not be processed for any purpose that is incompatible with that for which the information was collected. However, the processing of personal data for historical, statistical or scientific purposes shall not be regarded as incompatible with the purposes for which the information was collected. In accordance with the DPA, personal data processed solely for archival purposes in the public interest may be used to take action with respect to the data subject only if there are exceptional reasons with regard to the vital interests of the data subject. Public authorities may, however, process such personal data contained in public documents.

Security

20 Security obligations

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

A controller of personal data must, in accordance with article 32 of the GDPR, implement appropriate technical and organisational measures to protect the personal data that is processed.

The DIB does not impose detailed security obligations. However, it has published non-binding guidelines suggesting security measures such as adopting an information security policy and performing vulnerability and risk assessments.

21 Notification of data breach

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 article 33 of the GDPR, the controller shall in the event of a personal data breach without undue delay notify the competent supervisory authority and, where feasible, not later than 72 hours after having become aware of the breach. There is, however, no notification requirement if the breach is unlikely to result in a risk to 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 controller shall under article 34 of the GDPR communicate the personal data breach to the data subject without undue delay.

There is a requirement in the Electronic Communications Act for providers of public electronic communications services to notify PTS (the telecom NRA) of what the Act terms privacy incidents. If the incident can be expected to have a negative effect on the subscribers and users concerned, or on PTS's request, these subscribers and users must also be notified. Providers are required to maintain an updated register of privacy incidents their service has suffered.

PTS has adopted supplementary regulations on notification of privacy incidents and published a guideline on the notification requirement.

Public authorities under the central government are required under the Ordinance (2015:1052) on crisis preparedness and sector-responsible authorities actions at heightened states of readiness to adroitly report to the Swedish Civil Contingencies Agency (MSB) the occurrence of any IT incident in the authority's information system that may seriously affect the security of the information management for which the authority is responsible, or regarding a service the authority provides for another organisation. MSB has issued Regulations (MSBFS 2016:2) on how the reporting requirement for public authorities is to be fulfilled.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

In accordance with article 37 of the GDPR, controllers and processors are required to appoint a data protection officer where the processing is carried out by a public authority or other public body, or where the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale, or finally, where the core activities of the controller or the processor consist of processing on a large scale of sensitive personal data as categorised in article 9 or such personal data relating to criminal convictions and offences referred to in article 10.

While the GDPR elaborates on the position and tasks of the data protection officer, the only actual legal responsibility is to maintain the confidentiality requirement set out in the DPA.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Yes, under article 30 of the GDPR each controller, and where applicable the controller's representative, shall maintain a record of processing activities under its responsibility and of categories of such activities. This requirement does not apply to organisations employing fewer than 250 persons unless 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 such special categories of data as set out in articles 9 and 10.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Yes, under article 25 of the GDPR 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, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. Under article 35 of the GDPR, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There is no registration requirement under the GDPR or under national Swedish law.

26 Formalities

What are the formalities for registration?

Not applicable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

No.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Article 29 of the GDPR states that a processor and a person or those persons who work under the processor's or the controller of personal data's direction may only process personal data in accordance with instructions from the controller. Under article 28, the controller may only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

There must be a written contract on the processing by the processor of personal data on behalf of the controller of personal data. Article 28 requires the contract to contain specific commitments by the processor as set out in the article.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Any disclosure of personal data to other recipients must have an applicable legal basis under article 6 of the GDPR. Information about the disclosure must be given to the data subject under articles 13 and 14 of the GDPR.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Transfer of personal data that is undergoing or is intended for processing to a third country (outside of the EU/EEA) is prohibited under the GDPR unless the third country has an adequate level of protection for personal data. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding the transfer. Particular consideration shall be given to the nature of the data, the purpose of the processing, the duration of the processing, the country of origin, the country of final destination and the rules that exist for the processing in the third country.

Notwithstanding this prohibition, it is, however, permitted under the DPA to transfer personal data to a third country if the data subject has given his or her consent to the transfer, or if the transfer is necessary for:

- the performance of a contract between the data subject and the controller of personal data or the implementation of precontractual measures taken in response to the request of the data subject;

Update and trends

All data protection-concerned eyes in Sweden are keeping a close watch on what enforcement actions under the GDPR will be taken by the DIB, the new European Data Protection Board and the major EU member states' data protection supervisory authorities. Even though the great majority of Sweden's private and public sector organisations have put significant efforts into achieving GDPR compliance, few of these will feel complete confidence that they have achieved this status. Furthermore, a not insignificant number of organisations have considerable work remaining before they achieve at least a respectable level of compliance. Only the potentially severe sanctions under the GDPR and the increased general awareness of privacy and data protection issues could have brought on the improvements in data protection compliance that have occurred, but the degree to which compliance will be maintained remains to be proven.

- the conclusion or performance of a contract between the controller and a third party that is in the interest of the data subject;
- the establishment, exercise or defence of legal claims; or
- the protection of vital interests of the data subject.

It is also possible to transfer personal data to:

- countries recognised by the European Commission as having the same level of protection as the EU;
- any other country, if the contractual clauses approved by the European Commission have been incorporated in a contract between the two entities; and
- a company belonging to the same group as the data controller and in which binding corporate rules (BCRs) have been implemented, if the BCRs have been approved by the DIB.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No.

36 Further transfer

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.

Rights of individuals

37 Access

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

Under article 15 of the GDPR, the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to the personal data. The information shall be provided in writing or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. The information shall be provided without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

While the information shall as a general rule under article 12 be provided free of charge, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee taking into account the administrative costs of providing the information or refuse to act on the request.

Information does not need under the DPA to be provided about personal data in running text that has not been given its final wording when the application was made or that comprises an aide memoire or similar. However, this does not apply if the data has been disclosed to a third party or if the data was only processed for historical, statistical or scientific purposes or, as regards running text that has not been given its final wording, if the data has been processed for a longer period than one year.

To the extent that it is specifically prescribed by a statute or other enactment or by a decision that has been issued under an enactment that information may not be disclosed to the data subject, the right to information is curtailed. A controller of personal data that is not a public authority may in a corresponding case as referred to in the Public Information and Secrecy Act (2009:400) refuse to provide information to the data subject.

38 Other rights

Do individuals have other substantive rights?

Individuals have under certain circumstances under the GDPR articles 15 to 22 the right to object, require rectification, blocking or erasing as applicable of personal data. The controller must also notify a third party to whom the data has been disclosed about the measure, unless it is shown to be impossible or would involve a disproportionate effort.

The data subject is entitled at any time to revoke consent that has been given in those cases where the processing of personal data is only permitted on the basis of consent.

39 Compensation

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 controller of personal data is liable to compensate the data subject for damages as well as for the experience of violation of personal integrity that the processing of personal data in contravention of the DPA has caused.

The liability to pay compensation may, to the extent that it is reasonable, be adjusted if the person providing personal data proves that the error was not caused by him or her.

The amounts that have been awarded by the Swedish courts are typically in the hundreds of euros, in a few cases reaching as high as €3,000 to €5,000. The Swedish Supreme Court, in a ruling on 6 December 2013, awarded a plaintiff 3,000 kronor in damages when the defendant had published a verdict in a claims case on the internet without removing the plaintiff's name and address, writing that the standard compensation should apply. On 7 May 2014, the government's Office of the Chancellor of Justice awarded a person 5,000 kronor in compensation for his personal data being entered into an unlawfully maintained 'Traveller Registry' that listed persons of Roma ethnicity. The Stockholm District Court on 10 June 2016 awarded 11 plaintiffs a further 30,000 kronor each in damages with regard to the plaintiffs' personal data having been included in the Traveller Registry. The government as defendant appealed this latter award as too high, but the District Court's ruling was affirmed by the Svea Court of Appeal on 28 April 2017.

40 Enforcement

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

An individual's rights to damages and compensation are exercised through the court system. Other rights are enforced by the DIB, whose decisions may be appealed to a court.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The GDPR and the DPA do not apply to the extent that these regulations would conflict with the constitutional Freedom of the Press Act or the Fundamental Law on Freedom of Expression. Articles 5 to 30 and 35 to 50 of the GDPR, together with Chapters 2 to 5 of the DPA, do not

apply to the processing of personal data for journalistic purposes or for academic, artistic or literary creation.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, all orders by the DIB may be appealed to the Stockholm Administrative Court.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Sweden passed the amendments of 2010 to the EU electronic communications regulatory regime into law by an Act of the Riksdag on 17 May 2011. The new regulations came into force on 1 July 2011. Among the changes to the Electronic Communications Act (2003:389) was the 'cookie regulation'.

Chapter 6, section 18 of the Electronic Communications Act states that information may be stored in or retrieved from a subscriber's or user's terminal equipment only if subscribers or users are provided with access to information on the purpose of the processing and consent to the processing. This does not apply to the storage or retrieval necessary for the transmission of an electronic message over an electronic communications network, or for the provision of a service explicitly requested by the subscriber or user.

The preparatory work to the new legislation emphasises that internet users should not be inconvenienced through cumbersome routines relating to the use of legitimate tools such as cookies. This work suggests that consent to cookies may be expressed through web browser settings, but stops short of explicitly stating that browser settings are sufficient.

A broad alliance of industry organisations and online international and domestic companies has collaborated on a code of conduct for cookie use. A 'Recommendation on the use of cookies and comparable technology' was published in November 2011.

The supervisory authority to the Electronic Communications Act, the PTS, initiated an investigation in February 2014 into how cookies are used, writing to 16 organisations with popular websites (banks, media companies and public authorities) asking questions on cookie law compliance. Following extensive consultations with the concerned sites, the PTS on 27 June 2016 closed the investigation without bringing any charges or imposing any sanctions. The PTS promised to relay the results of the investigation into official guidance on the use of cookies, but has not provided any date for when guidance will be adopted. Draft guidance was circulated for comment in 2016, but no final guidance had been issued by 11 June 2018.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

The Marketing Act (2008:486) has regulations on marketing by email, fax or telephone.

Under the Marketing Act, a trader may, in the course of marketing to a natural person, use electronic mail, a telefax or automatic calling device or any other similar automatic system for individual communication that is not operated by an individual, only if the natural person has consented to this in advance.

Where a trader has obtained details of a natural person's electronic address for electronic mail in the context of a sale of a product to that person, the consent requirement shall not apply, provided that:

- the natural person has not objected to the use of the electronic address for the purpose of marketing via electronic mail;
- the marketing relates to the trader's own similar products; and
- the natural person is clearly and explicitly given the opportunity to object, simply and without charge, to the use of such details for marketing purposes, when they are collected and in conjunction with each subsequent marketing communication.

In marketing via electronic mail, the communication shall at all times contain a valid address to which the recipient can send a request that the marketing cease. This also applies to marketing to a legal person.

A trader may use methods for individual distance communication other than those referred to above, unless the natural person has clearly objected to the use of such methods.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

The GDPR also applies to the use of cloud computing services; there is no regulation specific to such services. The DIB has issued guidance on the subject, a four-page pamphlet titled 'Cloud services and the Personal Data Act' (also published in English). The guidance emphasises that whoever appoints a cloud provider is the controller of personal data and that the controller must carry out a risk and impact assessment with regard to engaging the provider. The DIB reminds cloud service users that when processing sensitive personal data (eg, information about health), information about legal offences and secrecy-protected information, the DIB requires that strong authentication be used when transferring data in an open network and that the data shall be protected by encryption. When such information is processed, the requirement for access checks often means that the controller of personal data shall not only carry out checks for particular reasons but also regularly and systematically follow up who has had access to which information. The DIB also stresses the importance of entering into an adequate processor agreement that complies with DPA requirements. The DIB has previously raised objections to processor agreements used by Microsoft Azure and Google Apps services.

W S A
L A W

Henrik Nilsson **henrik.nilsson@wsa.se**

Kungsgatan 36, PO Box 7836
Stockholm 10398
Sweden

Tel: +46 8 407 88 00
www.wsa.se

Switzerland

Lukas Morscher and Leo Rusterholz

Lenz & Staehelin

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Switzerland has dedicated data protection laws. On the federal level the Federal Data Protection Act (DPA) of 19 June 1992, together with its Ordinance (DPO) of 14 June 1993, governs processing of what in Switzerland is called 'personal data' by private parties or federal bodies. Processing of PII 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 (such as financial markets and telecommunications), which further address the collection and processing of PII:

- the Swiss Federal Code of Obligations (Code of Obligations) sets forth restrictions on the processing of employee data, and Ordinance 3 to the Swiss Federal Employment Act (Employment Act) limits the use of surveillance and control systems by the employer;
- the Swiss Federal Telecommunication Act (Telecommunication Act) regulates the use of cookies;
- the Swiss Federal Unfair Competition Act regulates unsolicited mass advertising by means of electronic communications such as email and text messages;
- statutory secrecy obligations, such as banking secrecy (set forth in the Swiss Federal Banking Act (Banking Act)), securities dealer secrecy (set forth in the Swiss Federal Stock Exchange and Securities Dealer Act (Stock Exchange Act), financial market infrastructure secrecy (set forth in the Swiss Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (the Financial Market Infrastructure Act)) and telecommunications secrecy (set forth in the Telecommunication Act) apply in addition to the DPA;
- the Banking Act, the Stock Exchange Act and the Swiss Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector stipulate specific duties to disclose information; and
- the Swiss Federal Act regarding Research on Humans, the Swiss Federal Act on Human Genetic Testing and the Swiss Federal Ordinance on Health Insurance set out specific requirements for the processing of health-related data.

Switzerland is a member state 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 ETS 108) and its additional protocol of 8 November 2001.

Although Switzerland is not a member of the EU and, hence, has neither implemented the EU Data Protection Directive 95/46/EC nor is directly subject to the EU General Data Protection Regulation 2016/679 (GDPR), it has been officially recognised by the European Commission as providing an adequate level of protection for data transfers from the EU.

A revision of the DPA (see 'Update and trends') shall align the DPA with international rules on data protection in order to comply with the upcoming revision of Convention ETS 108 and the GDPR. This will allow Switzerland to uphold its status as a country adequately protecting personal data from an EU perspective, which allows for easier transfer of personal data from the EU and to ratify Convention ETS 108 of the Council of Europe.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Federal Data Protection and Information Commissioner (FDPIC) is the federal data protection authority in Switzerland. In addition, cantons are competent to establish their own data protection authorities for the supervision of data processing by cantonal and communal bodies. The FDPIC's contact details are as follows:

Federal Data Protection and Information Commissioner
Feldeggweg 1
3003 Berne
Switzerland
Tel: +41 58 462 43 95
Fax: +41 58 465 99 96
www.edoeb.admin.ch

The FDPIC has no direct enforcement or sanctioning powers against private bodies processing PII. 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 (system errors), if data collections must be registered (see question 25) or if there is a duty to provide information in connection with a cross-border data transfer (see question 35). To this effect, the FDPIC may request documents, make inquiries and attend data processing demonstrations. On the basis of these investigations, the FDPIC may recommend that a certain method of data processing be changed or abandoned. However, these recommendations are not binding. If a recommendation made by the FDPIC is not complied with or is rejected, he or she may refer the matter to the Federal Administrative Court for a decision. The FDPIC has the right to appeal against such decision to the Federal Supreme Court.

The draft of the revised DPA (see 'Update and trends') foresees that the FDPIC may upon investigation issue binding administrative decisions (instead of recommendations under the current DPA), for example, to modify or terminate unlawful processing.

3 Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with 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 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) as regards supervision and control of processing activities or to share information with them. A collaboration of the FDPIC with foreign data protection authorities in relation to data processing in specific cases may (with the exception of 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).

As already mentioned, 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 (N-SIS-Ordinance) explicitly foresees a collaboration of the FDPIC with Swiss cantonal data protection authorities as regards coordinated supervision of PII 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.

4 Breaches of data protection

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 (see question 11) are generally not criminally sanctioned. However, private persons are liable to a fine of up to 10,000 Swiss francs if they wilfully:

- fail to provide information with regard to safeguards in the case of cross-border data transfers or to notify data collections or in so doing wilfully provide false information; or
- provide the FDPIC with false information in the course of an investigation or refuse to cooperate.

In addition, the wilful non-compliance with the following duties is, on complaint, punishable by a fine of up to 10,000 Swiss francs:

- the data subject's right of access by refusing to allow access or by providing wrong or incomplete information;
- the duty to inform the data subject on the collection of sensitive PII or personality profiles; and
- the duty of confidentiality of certain professionals to keep sensitive PII and personality profiles.

The draft of the revised DPA (see 'Update and trends') foresees a fine of up to 250,000 Swiss francs for the wilful breach of the obligations set forth above and further obligations set forth in the DPA. In contrast to the preliminary draft, a negligent breach is not intended to be sanctioned. Wilful breach of professional secrecy shall also be punishable by a fine of up to 250,000 Swiss francs. This new sanction will not be limited to the usual bearers of professional secrets (such as banks under article 47 Banking Act, securities dealers under article 43 Stock Exchange Act, financial market infrastructures under article 147 Financial Market Infrastructure Act or attorneys, auditors, doctors, etc, under article 321 Swiss Penal Code) but extend to any profession for which protection of confidentiality is essential.

Scope

5 Exempt sectors and institutions

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

The 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, with the exception of administrative proceedings of first instance;
- public registers based on private law;
- PII processed by state and communal bodies (regulated on state level); and
- PII processed by the International Committee of the Red Cross.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

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 Postal Traffic and Telecommunication;
- the Swiss Federal Act on the Intelligence Service;
- the Swiss Federal Unfair Competition Act;
- the Swiss Federal Code of Obligations; and
- Ordinance 3 to the Employment Act (regarding employee monitoring).

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Additional regulations concerning PII protection can be found in the following laws:

- the Swiss Federal Constitution;
- the Swiss Federal Civil Code;
- the Swiss Federal Act on Consumer Credits;
- Ordinance 3 to the Employment Act (regarding employee monitoring);
- various laws and other rules concerning banking (eg, the Anti-Money Laundering Act or the Outsourcing Circular, issued by the Swiss Financial Market Supervisory Authority (FINMA)); and
- various laws concerning health data (eg, the Swiss Federal Electronic Patient Records Act).

Further regulations may apply depending on the given subject matter.

8 PII formats

What forms of PII are covered by the law?

The DPA and DPO apply to any data relating to an identified or identifiable person (natural persons or legal entity), irrespective of its form. A person is identifiable if a third party having access to the data on the person is able to identify such person with reasonable efforts.

The draft of the revised DPA (see 'Update and trends') foresees to remove the protection of personal data relating to legal entities in order to ease cross-border disclosure to jurisdictions that do not protect respective personal data.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The DPA applies to any PII processing that occurs within Switzerland. In addition, 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 PII 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).

10 Covered uses of PII

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

The DPA applies to any processing of PII. 'Processing' is defined in the DPA as any operation with PII irrespective of the means applied and the procedure. In particular, processing includes the collection, storage, use, revision, disclosure, archiving or destruction of PII. An exemption is made for PII that is processed by a natural person 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 personal data are equally subject to the provisions in the DPA and the DPO and have to adhere to the rules set out therein.

Legitimate processing of PII

11 Legitimate processing – grounds

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

PII 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 DPA or non-compliance with these general principles is justified. The disclosure of PII to third parties is generally lawful under the same conditions. The principles set out in the DPA are:

- PII must be processed lawfully;
- the processing must be carried out in good faith and must be proportionate;
- the collection of PII and, in particular, the purpose of its processing, must be evident to the data subject at the time of collection;
- PII 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 PII must ensure it is accurate;
- PII must be protected against unauthorised processing through adequate technical and organisational measures;
- PII 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
- PII 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 the Banking Act); or
- an overriding private or public interest.

According to the DPA, an overriding interest of the person processing the PII can, in particular, be considered if that person:

- processes PII directly related to the conclusion or the performance of a contract and the PII is that of the contractual party;
- processes PII about competitors without disclosing it to third parties;
- processes PII that is neither sensitive PII nor a personality profile (for these categories, see question 12) in order 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 PII on a professional basis exclusively for publication in the edited section of a periodically published medium;
- processes PII for purposes not relating to a specific person, in particular for the purposes of research, planning statistics, etc, provided that the results are published in such a manner that the data subject may not be identified; and
- collects PII on a person of public interest, provided the data relates to the public activities of that person.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

In addition to 'normal' PII, the DPA introduced 'sensitive PII' and 'personality profiles' as special categories of PII that are subject to stricter processing conditions. Sensitive PII 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 PII that permits an assessment of essential characteristics of the personality of a natural person.

There are certain restrictions applying to processing sensitive PII 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, etc. (See questions 6 and 7.)

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Generally, it suffices if the collection of PII 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 PII 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 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 PII 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 in another recordable form.

The draft of the revised DPA (see 'Update and trends') foresees that the FDPIC must be notified in case of unlawful processing or loss of personal data (see question 21). The data subject shall also be informed about unlawful processing or loss of personal data if it is necessary to protect his or her privacy or if the FDPIC so requests. Further, the data subject shall be informed about automated decisions (ie, decisions taken solely on the basis of automated data processing) that have legal consequences or significantly affect him or her, and - under certain circumstances – be given the opportunity to comment on such decisions and processed PII.

14 Exemption from notification

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 own overriding interests justify not informing the data subject (in the latter case this exception only applies if the PII is not shared with third parties).

If the PII 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.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

See question 37 et seq.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Anyone who processes PII must ensure that the data is accurate and take all reasonable measures to ensure that PII, which, in view of the purpose of its collection is or has become incorrect or incomplete, is either corrected or destroyed.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Other than the general principle that processing of PII must be proportionate, there are no rules on amount or duration of its holding. According to this principle, processing may only be conducted in so far as it is necessary and fits the purpose for which PII is processed. The same applies to the duration. Accordingly, the permitted amount and duration must be assessed on a case-by-case basis.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

According to the DPA, PII may only be processed for the purpose stated or evident at the time of collection or that is provided for by law.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Use of PII 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 (see question 11).

Security

20 Security obligations

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

PII must be protected by appropriate technical and organisational measures against unauthorised processing. Anyone processing PII or providing a data communication network must ensure the protection against unauthorised access, the availability and the integrity of the data. In particular, the PII must be protected against the following risks:

- unauthorised or accidental destruction;
- accidental loss;
- technical faults;
- forgery, theft or unlawful use; and
- 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 taken into account:

- 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).

In relation to 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 PII is being processed;
- PII carrier control – preventing unauthorised persons from reading, copying, altering or removing data carriers;
- transport control;
- disclosure control – data recipients to whom PII is disclosed by means of devices for data transmission must be identifiable;
- storage control;
- access control – the access by authorised persons must be limited to the PII 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 PII was entered at what time and by which person.

The draft of the revised DPA (see 'Update and trends') foresees that appropriate measures shall be taken to avoid breaches of privacy (privacy by design) and data-protection-friendly presets shall be provided (privacy by default).

21 Notification of data breach

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 FDPIC has advised lawmakers to oblige providers of social networking sites to inform data subjects of data breaches.

The draft of the revised DPA (see 'Update and trends') foresees an explicit obligation of data breach notifications (see question 13).

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

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 FDPIC is notified of the appointment of a data protection officer. A list of such business organisations who 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 PII 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. The 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 in fact 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 to 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 dismissal of the data protection officer. The data protection officer can be an employee of the data controller or an external person.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Although the owner of a data collection may have to provide available information about the source of collected data (see question 37), there is no obligation to actually keep the according 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 draft of the revised DPA (see 'Update and trends') foresees a record-keeping obligation for both controllers and processors.

24 New processing regulations

Are there any obligations in relation to new processing operations?

In general, PII must be protected against unauthorised processing through adequate technical and organisational measures (see question 20); however, there is currently no obligation to carry out a privacy impact assessment.

The draft of the revised DPA (see 'Update and trends') foresees additional obligations in relation to new processing operations, such as appropriate measures to be taken to avoid breaches of privacy (privacy by design) and the carrying out of a privacy impact assessment under certain circumstances.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

The owner of a data collection that regularly processes sensitive PII or personality profiles, or regularly discloses PII to third parties, has the obligation to register such data collection with the FDPIC.

A data processor that transfers PII outside Switzerland is, under certain circumstances, obligated 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 PII owing to a statutory obligation;
- he or she uses the PII 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 DPO, including, among other things:
  - data collections of suppliers or customers, provided they do not contain any sensitive PII or personality profiles;
  - collections of PII that are used exclusively for research, planning and statistical purposes; and
  - accounting records.

26 Formalities

What are the formalities for registration?

In the case of a registration obligation, the collection has to be registered before it is created and the FDPIC has to 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 PII 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 PII in the data collection.

The owner of the data collection is under the obligation to keep the data collection registration up to date. Online registration is possible at www.datareg.admin.ch. No fees are charged for registration of a data collection.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Private persons 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.

The draft of the revised DPA imposes fines of up to 250,000 Swiss francs in case of breach of certain duties under the DPA (such as information, notification and cooperation duties, compliance measures, etc), including the failure to make or maintain an entry on the register (see question 4 and 'Update and trends'). In contrast to the preliminary draft, a negligent failure is no longer foreseen to be sanctioned.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Swiss law does not provide for the FDPIC to refuse an entry on the register.

29 Public access

Is the register publicly available? How can it be accessed?

The database of data collections registered with the FDPIC is publicly available and can be accessed by anyone free of charge via the internet at www.datareg.admin.ch. On request, the FDPIC also provides paper extracts free of charge.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Registering a data collection with the FDPIC does not have additional legal effects.

31 Other transparency duties

Are there any other public transparency duties?

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 (see questions 22 and 29 respectively), 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.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The processing of PII 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 PII solely for the purposes of, and only under the instructions of, the transferor.

Special rules may apply in regulated markets. Circular 2018/3 relating to outsourcing issued by the FINMA applies to banks and securities dealers with a registered office in Switzerland and Swiss branches of foreign banks and securities dealers, as well as insurance companies with a registered office in Switzerland and branches of foreign insurance companies requiring authorisation to commence business operations (initial authorisation) or authorisation for individual elements of the business plan (authorisation for changes). Before outsourcing a significant business area, these institutions must comply with the detailed measures set out in the circular, including:

- careful selection, instruction and monitoring of the service provider;
- assurance of the possibility of restructuring or resolving the company in Switzerland, ie, access to the information required for this purpose must be possible in (and not only from) Switzerland at all times; and
- conclusion of a written contract with the service provider setting out, among other things, the company's obligation to make the use of subcontractors (by the service provider) for significant functions contingent on its prior approval and measures to ensure implementation of the requirements as regards instruction and control rights, security, audit rights and cross-border outsourcing.

With FINMA's issuance of Circular 2018/3 (formerly Circular 2008/07), any references to data protection and customer-focused requirements (in particular with respect to comprehensive information duties and the extraordinary termination right) have been removed. Such aspects are now governed by the respective federal acts only.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

For general requirements regarding disclosing of PII, sensitive PII and personality profiles, see questions 11 and 12. It should be noted that even the communication of PII between companies belonging to the same corporate group is deemed to be disclosure of PII to third parties. Only transmission to an outsourcing provider (see question 32 for requirements) does not constitute such disclosure.

Regularly disclosing information contained in a PII collection entails a registration obligation for such collections.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

PII 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 FDPIC has published on its website a list of jurisdictions that provide adequate data protection (www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html). The EEA 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 as regards PII of individuals (however, many do not with regard to PII 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, PII may only be transferred outside Switzerland if:

- sufficient safeguards, in particular, contractual clauses, ensure an adequate level of protection abroad (see below for details);
- 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 PII 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 in order to protect the life or the physical integrity of the data subject;
- the data subject has made the PII 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 (see below for details).

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 provides a model data transfer agreement (owner of a data collection to a data processor), which can be accessed on its website. The model data transfer agreement is based on Swiss law and reflects to a large extent the standard contractual clauses of the European Commission for data transfers. Further, the FDPIC has pre-approved the European Commission's standard contractual clauses for data transfers and the model contract of the Council of Europe as safeguards, which provide adequate data protection, although it is unclear whether they must be adapted to also cover PII of legal entities and the protection of personality profiles.

An 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. BCRs should address at a minimum the elements covered by the model data transfer agreement provided by the FDPIC.

The draft of the revised DPA (see 'Update and trends') foresees BCRs to be approved (not only notified to the FDPIC).

The US–Swiss Safe Harbor Framework, established in 2009, was considered to provide adequate protection for the transfer of personal data from Switzerland to the US. In its decision of 6 October 2015, the CJEU held that the US–EU Safe Harbor Framework does not provide adequate protection for the transfer of personal data abroad. Even though that decision only concerns the US–EU Safe Harbor Framework and is not directly applicable to Switzerland, the FDPIC declared that the US-Swiss Safe Harbor Framework can no longer be considered to provide adequate protection.

In February 2017, Switzerland and the US agreed on a new framework for the transfer of personal data from Switzerland to the US called the Swiss–US Privacy Shield, thereby replacing the US–Swiss Safe Harbor Framework. US companies processing personal data may self-certify to the Swiss–US Privacy Shield with the US Department of

Update and trends

The DPA is still being revised and the Swiss parliament has decided to divide the ongoing revision into two parts, as follows:

- The first part includes the revision of only those provisions of the DPA that are required due to the implementation of Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (the Directive). The Directive must be implemented by Switzerland as it forms part of the Schengen acquis. The scope of the Directive is limited to the processing of personal data by competent authorities for the aforementioned purposes. Accordingly, it only imposes additional obligations on authorities conducting such processing as a controller and natural or legal persons processing personal data as a processor on behalf of such an authority. Thus, it is of less relevance for private companies.
- The second part of the DPA revision (ie, the revision of those DPA provisions necessary to uphold the EU adequacy decision for Switzerland, such as provisions introduced in the EU through the GDPR) will be taken up subsequently and the respective timing remains unknown, although it is currently expected that the second part of the revision will enter into force around late 2019 or early 2020.

Commerce and thus publicly commit to comply with the new framework. Switzerland acknowledges that the level of protection of personal data for such certified US companies is adequate. As a result, Swiss companies are able to transfer personal data to those US business partners without the need to procure the consent of each data subject or to put additional measures in place.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

As stated in question 34, PII may be transferred outside Switzerland to a jurisdiction that does not provide for adequate data protection based on safeguards that ensure adequate protection such as contractual clauses or binding corporate rules; however, the FDPIC must be notified of such safeguards. The FDPIC may, during a period of 30 days, review the safeguards, though the data transferor does not have to wait for the result of the FDPIC's review or obtain approval. Moreover, if PII is transferred outside Switzerland on the basis of safeguards that have been pre-approved by the FDPIC (eg, the model data transfer agreement issued by him or her), the FDPIC only has to be informed about the fact that such safeguards form the basis of the data transfers.

36 Further transfer

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, eg, the FDPIC's model data transfer agreement does).

Rights of individuals

37 Access

Do individuals have the right to access their personal information held by PII 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 PII 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 PII 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 PII processed;
- other parties involved with the data collection; and
- the recipients of the PII.

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 period, the owner of the data collection must inform the data subject of the time period 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 PII 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 prior to the request and no legitimate interest in the repeated provision of information can be shown, whereby, in particular, a modification of the PII 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.

38 Other rights

Do individuals have other substantive rights?

The DPA further provides for the following rights for data subjects:

- right of rectification;
- right of erasure; and
- right to object to the processing or disclosure of PII.

Further, if it is impossible to demonstrate whether PII 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.

39 Compensation

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 for the surrender of profits based on the violation of his or her privacy and may request that the rectification or destruction of the PII or the judgment be notified to third parties or be published.

40 Enforcement

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 (see question 2 for details on the FDPIC's competences).

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The most important derogations, exclusions and limitations have been mentioned above. As previously stated, depending on the subject matter, there may be additional regulations applicable that can have significant impact on the general data protection rules, adding to them, modifying them or even exempting them from application.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

The FDPIC's recommendations are non-binding, hence, there is no need for them to be reviewed by a judicial body. The verdicts of the Federal Administrative Court, which may ensue when the owner of a data collection refuses to follow such recommendation (see question 2), on the other hand, are appealable to the Federal Supreme Court both by the FDPIC as well as the defendant.

Specific data processing

43 Internet use

Describe 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 other online service), which installs the cookie on the user's computer (or other 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 or a 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.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

In 2007, Switzerland adopted a full consent opt-in regime with respect to unsolicited mass advertisement by means of telecommunications (eg, email, SMS/MMS, fax or automated telephone calls). Pursuant to 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 PII 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.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

There are no rules specifically applicable to cloud services. In general, personal data must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is stored. Anyone processing personal data must ensure its protection against unauthorised access, its availability and its integrity (see question 20). Further, the use of cloud services constitutes an outsourced processing service if the personal data is not encrypted during its storage in the cloud (for requirements in this regard, see question 32 et seqq) and, in case the servers of the cloud are located outside Switzerland and the personal data is not encrypted during its transfer and storage, an international transfer of personal data (for requirements in this regard, see question 34 et seq). Additionally, the FDPIC has issued a non-binding guide outlining the general risks and data protection requirements of using cloud services (www.edoeb.admin.ch/edoeb/en/home/data-protection/Internet_und_Computer/cloud-computing/guide-to-cloud-computing.html).

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, Brian, Hsiang-Yang Hsieh and Ruby, Ming-Chuang Wang

Formosa Transnational Attorneys at Law

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Taiwan has a one-piece legislation, the Personal Data Protection Act (PDPA), which affords comprehensive protection with respect to the use, collection and processing of PII by governmental agencies and private entities. The PDPA sets forth statutory requirements that must be met by the entities for the use, collection and processing of PII. Special protections are imposed upon an entity if the PII 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 liable; 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 Directive 95/46/EC, the OECD guidelines and the APEC privacy framework when drafting the PDPA.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The PDPA does not give any single governmental agency overriding authority to oversee enforcement of the PDPA. As such, there is no particular governmental agency in Taiwan that has been actively policing personal data protection practices. The PDPA, however, requires Taiwan's Ministry of Justice, equivalent to the US Department of Justice, to set forth guiding principles for all other governmental agencies, central and local, to take into account when enforcing the provisions of the PDPA.

3 Legal obligations of data protection authority

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

As noted above, the PDPA does not give any particular governmental agency overriding authority to enforce the data protection law. However, the PDPA does require the Ministry of Justice to set forth guiding principles.

4 Breaches of data protection

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 having 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 PII. The agency could also order the breaching entity to delete the PII possessed by the breaching entity, or to confiscate or destroy the PII 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 an amount 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$1,000,000.

Scope

5 Exempt sectors and institutions

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

The PDPA is applicable 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 PII. 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.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

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 PII as defined in the PDPA, the PDPA will certainly regulate said activity. Additionally, anyone conducting illegal surveillance will be in violation of 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.

7 Other laws

Identify 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 PII of participants who provide biological specimens. The Enforcement Rules for the Financial Technology Development and Innovative Experimentation Act (Sandbox Act) provide specific rules to manage and protect PII 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.

8 PII formats

What forms of PII are covered by the law?

The PDPA covers all PII without limitation to specific formats of personal data.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

No. Even if the use, collection or processing occurs outside the territory of Taiwan, the PDPA is applicable so long as the data subject is a Taiwan citizen.

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 PII of other Taiwan citizens outside the territory of Taiwan.

10 Covered uses of PII

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

Yes, the PDPA covers all processing and use of PII. The PDPA does not distinguish between those who control or own PII and does not impose different duties and obligations.

The definitions of PII collection, processing and use under the PDPA are as follows:

- collection: to collect PII in any form or in any way;
- processing: to record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit PII for the purpose of establishing or using a PII file; and
- use: to use PII in any way other than processing.

Legitimate processing of PII

11 Legitimate processing – grounds

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

According to the PDPA, a non-governmental entity (including natural persons and private agencies) may collect and process PII for a specific purpose in the following situations:

- the collection or processing of PII is permitted by law;
- the collecting or processing party and the PII subject (individual) form or are going to form a contractual relationship, and the collection and processing of PII is done with proper safety measures;
- the PII is published by the PII subject or is legally published by a third person;
- the collection or processing of the PII 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 PII has altered the PII such that the subject cannot be identified by the PII;
- the collection or processing is made with the PII subject's consent;
- the collection or processing of the PII is done to enhance the public interest;
- the PII is collected from publicly available resources; and
- the right or interest of the PII subject will not be harmed.

However, where the PII is collected from publicly available resources, the PII shall not be further collected or processed if the data subject objects to such collection.

Also, according to the PDPA, use of the PII will be permitted if such use is within the specific purpose for collecting and processing the PII.

Moreover, while requesting the PII subject's consent, the collecting party must disclose the following information:

- the name of the authority collecting the PII;
- the purpose of collection;
- the category of the PII;
- the period, area, object and method of use of the PII;
- the rights of the data subject to request a review of his or her PII, to make duplications of his or her PII, to supplement or correct his or her PII, to have the collection, processing or use of his or her PII discontinued and to have his or her PII deleted from the record; and
- the influence on his or her right 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 PII is necessary for a governmental agency to perform its official duties or for a non-government entity to fulfil a legal obligation;
- the disclosure will impede a governmental agency in performing its official duties;
- the disclosure will impair the public interest;
- the PII 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.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The PDPA does impose more stringent rules for specific types of PII. Sensitive PII, 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 PII is permitted by law;
- the collection, processing and use of PII is necessary for a governmental 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 PII;
- the PII is published by the PII subject (individual) or is legally published by a third person;
- the collection, processing or use of PII is made by a governmental or research entity for the purpose of enhancing medical treatment or health or to prevent criminal activities, where the collection, processing and use of PII is necessary to perform statistical or academic research, and where the collecting party or the providing party of such PII has altered the PII such that the individual cannot be identified;
- the collection, processing and use of PII is done to assist a governmental or non-governmental 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 PII; and
- to the extent permitted by law, the collection, processing and use of PII is made with the PII subject's written consent.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Yes, in accordance with the PDPA, if the PII is collected without the consent of the data subject, the PII owner is required to notify the data subject of its possession of his or her PII before the owner processes or uses the PII. The notice must include the following information:

- the source of collection;
- the name of the authority collecting, processing or using the PII;
- the purpose of the collection;
- the category of the PII;
- the period, area, object and method of use of the PII; and
- the rights of the data subject to request a review of his or her PII, to make duplications of his or her PII, to supplement or correct his or her PII, to have the collection, processing or use of his or her PII discontinued, and to have his or her PII deleted from the record.

14 Exemption from notification

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 PII is necessary for a governmental agency to perform its official duties or for a non-governmental entity to fulfil a legal obligation;
- giving notice will impede a governmental agency in performing its official duties;
- giving notice will impair the public interest;
- the PII 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 PII is published by the data subject or is legally published by a third person;
- the PII owner cannot inform the data subject or his or her representative;
- the processing or use of the PII 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 PII has altered the PII such that the individual cannot be identified; and
- the PII is collected by the mass media for the purpose of reporting news in the public interest.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The PDPA affords data subjects the right to request the PII owner to allow a review of his or her PII, to provide duplications of his or her PII, to supplement or correct his or her PII, to cease collecting, processing or using his or her PII, and to have his or her PII deleted from the record.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The PDPA does not set forth standards for the quality, currency and accuracy of PII. However, the PDPA requires the PII owner to maintain the accuracy of PII and to actively supplement or correct the PII, or to do so upon request by the data subject. Additionally, if the accuracy of the PII is in dispute, the PII owner must actively cease processing or using the PII or do so upon request by the data subject. However, if the processing or use of the PII is necessary to perform official duties or to fulfil legal obligations, or is consented to by the data subject, the PII owner may continue its processing or use of the PII after recording that the PII is in dispute.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The PDPA does not restrict the amount of PII that may be held or the specific length of time it may be held. Nevertheless, the PDPA requires the PII owner to cease processing or using the PII once the specific purpose of the collection, processing or use of the PII no longer exists or the term of such purpose has expired. However, if processing or using the PII is necessary to perform official duties or to fulfil legal obligations, or is consented to by the data subject, the PII owner may continue to process or use the PII.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes, the purposes for which PII can be used are restricted by the PDPA. The PDPA provides a 'finality principle' under which the rights and interests of data subjects must be respected while the PII owner collects, processes or uses PII, and any collection, processing or use of PII must be conducted in good faith, must not go beyond specific purposes and must be performed in connection with the purpose of the collection.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Yes, there are some exceptions from the finality principle. The PDPA allows PII to be used for new purposes if any one of the following situations exists:

- using PII for a new purpose is permitted by law;
- using PII for a new purpose is done to enhance a public interest;
- using PII for a new purpose is to prevent harm to the life, body, freedom or property of the data subject (individual);
- using PII for a new purpose is to prevent harm to the rights and interests of other people;
- PII is used by a research entity or governmental agency where using the PII 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 PII has altered the PII so that the individual cannot be identified;
- using PII for a new purpose is agreed to by the data subject; and
- using PII for a new purpose will benefit the rights of the data subject.

However, none of these exemptions applies to any sensitive data.

Security

20 Security obligations

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

A governmental agency or non-governmental entity keeping possession of any PII must adopt appropriate cybersecurity measures to prevent the PII from being stolen, altered, damaged, destroyed or disclosed. If the PII owner is a governmental agency, such agency is required to assign specific persons to be in charge of the security of PII. Also, the PDPA Enforcement Rules provide guidelines for such security measures. For example, the PII owner may assign and allocate personnel to manage PII, establish a mechanism to evaluate risk, to prevent leaks, to 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-governmental entities to stipulate internal principles to protect the safety of PII, including how PII will be disposed of after the termination of the relevant business.

21 Notification of data breach

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 PII owners to notify data subjects of any data breaches if a breach results in PII being stolen, altered, damaged, destroyed or disclosed. In addition, some relevant PII regulations specifically applied to particular industries also require PII owners to report data breaches to the relevant governmental authorities. For example, PII owners in the banking and insurance industries are required by the regulations made by the Financial Supervisory Commission (FSC) to report data breaches to the FSC.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

In accordance with the PDPA, a governmental agency keeping possession of PII is required to appoint a data protection officer, but this does not apply to a non-governmental entity. The responsibility of the data protection officer is to prevent PII from being stolen, altered, damaged, destroyed or disclosed. However, the guidelines for security measures afforded by the PDPA Enforcement Rules suggest that a non-governmental entity appoint a data protection officer to manage the PII that it possesses. In addition, some relevant PII regulations specifically applied to particular industries also require PII owners to appoint a data protection officer. For example, the regulations applicable to banks, insurance providers and short-term educational centres require entities in these industries to appoint a data protection officer.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The PDPA does not require PII owners or processors to maintain internal records of their processing or use of PII. However, the PDPA Enforcement Rules suggest that PII owners or processors, whether governmental or non-governmental entities, keep internal records to protect the security of PII. On the other hand, some relevant PII regulations specifically applicable to particular industries require PII owners or processors to maintain internal records of the use of PII. For example, the regulations made by the FSC require PII owners in the banking and insurance industries to maintain such internal records.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The PDPA does not address approaches for privacy-by-design or risk assessments for privacy impacts. However, the PDPA Enforcement Rules suggest that PII owners or processors, whether governmental or non-governmental entities, establish a mechanism to evaluate the risk of collecting, processing and using PII. Some relevant PII regulations specifically applied to particular industries, however, require PII owners or processors to periodically make risk assessments on their collecting, processing or use of PII. For example, online shops and platforms, banks and insurance providers, real estate agencies and short-term educational centres are obligated to make such PII risk assessments.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

PII owners or processors are not required to register with the supervising authority before carrying out the collection, processing or use of PII.

26 Formalities

What are the formalities for registration?

Not applicable.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

29 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

30 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

31 Other transparency duties

Are there any other public transparency duties?

In accordance with the PDPA, a governmental agency is required to publish the following information on the internet or by other proper means for review:

- the name of a PII file;
- the name of the governmental entity keeping the PII file and its contact information;
- the legal basis for and purpose of keeping the PII; and
- the classification of PII.

Non-governmental entities keeping PII are not obligated to make such publication.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

There is no provision of the PDPA specifically regulating the transfer of PII to entities that provide outsourced processing services. However, because the transfer of PII is categorised as an activity of processing or using PII under the PDPA, the transfer of PII to entities that provide outsourced processing services must comply with all provisions regulating the processing or use of PII. As such, while transferring PII to another entity, the PII owner is obligated to prevent the PII from being stolen, altered, damaged, destroyed or disclosed.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosing PII to other recipients must be done in accordance with the regulations for the use of PII under the PDPA. That is, for a non-governmental entity, if disclosing PII to other recipients is within the scope of a specific purpose for collecting and processing the PII, the PII owner may freely make such disclosure. Otherwise, the disclosure can be made only if it satisfies the requirements under which the use of PII for new purposes is allowed. However, the recipient must notify the data subject of its possession of PII before processing or using the PII. For the requirements of using PII for new purposes and contents of notification given by the recipients and their exceptions, see questions 19, 12 and 13.

Update and trends

As modern business goes digital and international, the EU's General Data Protection Regulation (GDPR), effective on 25 May 2018, has had a great impact on many Taiwan entities doing business with European entities. Compared to the PDPA in Taiwan, the GDPR provides more details as to the requirements for the protection of personal data. The significant penalty that the GDPR imposes is also something to which a market player must pay close attention. As such, increasingly more Taiwan enterprises are preparing for the application of the GDPR and have established proper internal data protection mechanisms, which reflect the fact and reality of globalisation.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The PDPA does not impose restrictions on international transfers of PII by governmental entities, but non-governmental entities are restricted by central government from transferring PII 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 PII will be received lacks proper regulations on the protection of PII and the transfer might harm the rights and interests of data subjects; or
- the international transfer of PII is made to evade the provisions of the PDPA.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, the PDPA does not require notification to or authorisation from a supervisory authority before or after engaging in a cross-border transfer of PII. However, because the central government may restrict non-governmental entities from transferring PII to other jurisdictions, as provided by the PDPA, it is prudent to confirm the legality with the supervisory authority before making any international transfer of PII.

36 Further transfer

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-governmental entities without differentiation between service providers or PII owners.

Rights of individuals

37 Access

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

Yes, the PDPA gives data subjects the right to access their personal information held by PII owners. Data subjects may request PII owners to allow a review of their PII or to provide duplications of their PII. However, under 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 PII owner or a third person.

38 Other rights

Do individuals have other substantive rights?

In addition to the data subject's right to request PII owners to allow a review of his or her PII or to provide duplications of his or her PII, 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 PII, and to delete his or her PII. These rights of data subjects cannot be waived by data subjects.

39 Compensation

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 PII is breached. Below are the details:

(i) 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 PII subject is harmed due to the PII owner's breach of the PDPA, the PII subject may request the court to order the PII owner to restore his or her reputation.

(ii) 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.

(iii) 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$200,000,000. However, if the value of the interests the breaching party may gain from the alleged violation is higher than NT$200,000,000, the victims are entitled to monetary compensation of no more than the established value of said interests.

(iv) If the damages to multiple data subjects by the same cause and fact exceed NT$200,000,000, the limitation on compensation granted of the amount of no less than NT$500, as provided under the condition specified at (ii) above, shall not apply.

(v) 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(s) 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-governmental entity, the entity may be free from liability if the entity successfully shows that the breach occurred without intent or negligence.

40 Enforcement

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 PII owner is a non-governmental entity may go to the courts or report the matter to a governmental agency having proper jurisdiction.

If the PII owner is a governmental agency, data subjects must file an administrative appeal against said governmental agency and, if not successful, then file an administrative lawsuit.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The PDPA will not apply where the collection, processing and use of PII by a person is merely for personal and family activity, as well as where audio-visual information is collected, processed or used in public places or in public activities without association to other personal information (such as video recorded by dashboard cameras).

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, if the PII owner believes an order of a supervisory authority is in error, it may first appeal the order to its superior authority and then, if not successful, to the administrative court. However, for orders made by a supervisory authority mandating that the PII be detained or duplicated, the PII owner may directly file an objection to the supervisory authority at the time these orders are issued.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The PDPA does not contain specific provisions to regulate the use of cookies. However, if the information collected through cookies matches the definition of PII, the PDPA shall apply. Taking distributing targeted advertisements, for example, when the server collects PII from an individual, it must comply with the rules regulating PII collection under the PDPA; when the server analyses the PII collected, it must comply with the rules regulating PII processing and use under the PDPA; when the server uses its analysing report to distribute targeted advertisements, it must comply with the rules regulating PII 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 PII when the user visits the website for the first time.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

In accordance with the PDPA, when a non-governmental entity uses the PII collected to do marketing, regardless of whether it's via email, fax or telephone, it must cease doing the same if the data subject so requires. Also, when PII is first used by a non-governmental 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 said entity.

45 Cloud services

Describe 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. The use of cloud computing services must comply with all rules regulating the collection, processing and use of PII 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 between each other. As such, in accordance with 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 of and time 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. See question 34 for regulation on cross-border transfers of PII.

萬國法律事務所
Formosa Transnational
SINCE 1974 Attorneys at Law

Yulan Kuo **yulan.kuo@taiwanlaw.com**
Jane Wang **jane.wang@taiwanlaw.com**
Brian, Hsiang-Yang Hsieh **brian.hsieh@taiwanlaw.com**
Ruby, Ming-Chuang Wang **ruby.wang@taiwanlaw.com**

13F Lotus Building,
136 Jen Ai Road,
Section 3,
Taipei 10657,
Taiwan

Tel: +886-2-2755-7366
Fax: +886-2-2708-8435
www.taiwanlaw.com

Turkey

Ozan Karaduman and Selin Başaran Savuran

Gün + Partners

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The protection of personally identifiable information in Turkey is regulated mainly by the Law on the Protection of Personal Data (DPL), which came into effect on 7 April 2016. The DPL is heavily modelled on Directive 95/46/EC, with many of the terms and central provisions very closely mirroring their equivalents in the Directive. Other than the DPL, there are a few other central legislative measures that constitute the framework of the protection of PII in Turkey.

The first of these is the Turkish Constitution, article 20 of which defines and enshrines the right to the protection of personal data. The Turkish Criminal Code also contains provisions relating to the unlawful recording and obtaining of personal data. In fact, before the introduction of the new DPL, the data protection regime in Turkey was based primarily on the relevant articles of the Constitution and the Turkish Criminal Code.

While the DPL provides the central framework for the general data protection regime in Turkey, there are also certain industry-specific regulatory measures that introduce further requirements. The most prominent examples of such industry-specific measures are those relating to the electronic communication and banking sectors.

Furthermore, the Turkish Data Protection Authority (Turkish DPA) issued ancillary legislation, such as the Regulation on Data Controller Registry (Regulation on Registry), the Regulation on Deletion, Destruction and Anonymisation of Personal Data, the Communiqué on Procedures and Principles for Application to Data Controllers and other guidelines and principle decisions.

In addition to these national legislative and regulatory measures, Turkey is also a signatory to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. While a signatory since 28 January 1981, Turkey only ratified the Convention on 2 May 2016.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The implementation of the DPL has been granted to the Turkish DPA. The DPL contains provisions regarding both the establishment of the Turkish DPA and the scope of its powers and responsibilities. Accordingly, as per the DPL, the Turkish DPA has been granted investigative powers in order to ascertain whether data controllers and data processors are in compliance with the provisions of the DPL. To this end, the Turkish DPA may conduct investigations (either upon complaint or ex officio) in order to evaluate whether data processing is being conducted in compliance with the DPL and, if necessary, implement any temporary preventative measures. Furthermore, the Turkish DPA has been tasked with reviewing and ruling on any referred complaints alleging the violation of the fundamental data protection rights.

In light of the DPL, the Turkish DPA was established and commenced its operations in January 2017. Since that date, the Turkish DPA has issued several ancillary regulations, guidelines and principle decisions supplementing the implementation of the DPL. Furthermore, the Turkish DPA has started to investigate complaints regarding the violation of data protection legislation and issued decisions concerning these violations where it has imposed administrative fines.

3 Legal obligations of data protection authority

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

There is no data protection authority other than the DPA in Turkey. There is not an explicit obligation of the Turkish DPA to cooperate with data protection authorities in other countries. However, pursuant to the DPL, the Turkish DPA is responsible for cooperating with public institutions and organisations, non-governmental or professional organisations or universities when needed, as well as being responsible for cooperating with international organisations and participating in meetings on matters that fall under its scope of duty.

4 Breaches of data protection

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

As per the DPL, the breach of the provisions can lead to both administrative fines and criminal penalties. With regard to potential criminal penalties, the DPL itself makes reference to the relevant measures of the Turkish Criminal Code that detail unlawfully recording or accessing personal data. As per article 135 of the Turkish Criminal Code, unlawful recording of personal data can be sanctioned with a one- to three-year prison sentence; with the sanction being increased by half should the unlawfully recorded personal data be personal data of a sensitive nature. Article 136 states that unlawfully obtaining or transferring personal data is punishable by a two- to four-year prison sentence. Finally, article 138 of the Turkish Criminal Code states that those persons who have kept and not erased personal data beyond the period stipulated by DPL can be sanctioned with a prison sentence of one to two years.

In addition to criminal proceedings, the DPL also establishes administrative fines that may be applied in the situation of a breach. There are four main breaches that have been defined in the context of a potential administrative fine:

- a data controller not satisfying their obligation to inform the data subject;
- the data controller not satisfying the data security requirements;
- the data controller not implementing the decisions of the Turkish DPA; and
- the data controller not satisfying their obligation to register on the Data Controller Registry (the Registry).

These breaches can be sanctioned with administrative fines ranging from 5,000 to 1 million liras.

Depending on the nature of the breach – as in whether the breach constitutes a criminal or administrative offence – the data controller will either be referred to the prosecutor or the Turkish DPA or both.

Scope

5 Exempt sectors and institutions

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

The DPL does contain a provision that defines areas and activities of exception where the provisions of the DPL will not be applied. These areas of exception are as follows:

- use of personal data by real persons within the scope of activities relating to either themselves or their family members living in the same house; on the condition that the data is not provided to third parties and data security requirements are followed;
- processing of personal data for official statistics or – on the condition that the data is made anonymous – used for purposes such as research, planning or statistics;
- on the condition that such use is not contrary to national defence and security, public safety and order, economic security, the right to privacy and personal rights, and on the condition that it does not constitute a crime, processing for the purposes of art, history, literature or scientific pursuits or processing within the scope of the freedom of speech;
- processing within the scope of the preventive, protective and intelligence activities of the public bodies and institutions that have been authorised by law to safeguard national defence, security, public safety and order or economic security; and
- processing by judicial authorities or penal institutions in relation to investigations, prosecutions, trials or enforcement proceedings.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The DPL does not cover the issues of interception of communications, electronic marketing or the monitoring and surveillance of individuals.

The areas of interception of communications and the monitoring and surveillance of individuals are primarily regulated by the Turkish Criminal Procedure Code. The specifics of these areas are further regulated with more specific regulatory measures such as the Regulation on Inspection of Communication made via Telecommunication, Undercover Investigations and Surveillance with Technical Tools due to the Law of Criminal Procedure.

The legislative measures that regulate the electronic communication sector, primarily the Electronic Communication Law (ECL) and ancillary regulations such as the Authorization Regulation also specify that licensed operators operating within the electronic communication sector are under the obligation to establish and maintain the infrastructure that will enable such lawful interception and surveillance activities.

Electronic marketing is covered by the Law on the Regulation of Electronic Commerce (E-Commerce Law) and its ancillary regulations.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

The primary sector-specific laws and regulations that introduce further data protection rules can be found in the electronic communication and banking sectors.

With regard to the electronic communication sector, the ECL introduces specific rules regarding how licensed operators operating in this sector may use traffic and location data that they can obtain from their customer. Furthermore, the Regulation on the Processing of Personal Data in the Electronic Communication Sector and the Protection of Privacy also contains further sector-specific rules regarding data processing in the electronic communication sector.

Certain legislative measures such as the Law on Payment and Security Agreement Systems, Payment Systems and Electronic Currency Organisations, requires financial institutions to keep their primary and secondary systems within Turkey and thus prevent transfer of such data abroad. Furthermore, the Banking Law introduces specific confidentiality obligations for persons who, owing to their position and task, are in possession of secret information relating to banks or their client. The Law on Bank Cards and Credit Cards imposes a similar obligation on this industry.

8 PII formats

What forms of PII are covered by the law?

The DPL defines personal data widely as 'all information relating to an identified or identifiable real person'. Furthermore, the DPL does not make any limitations or distinctions with regard to the format that such PII is maintained or stored. Therefore, in light of the central definition of the DPL, it can be said that the forms of PII covered are extensive both in the nature of the information and in terms of the format.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

While the DPL does not have a specific geographic scope that is stated within the text of the Law, it should be noted that as a Turkish law with sanctions applied by either Turkish public bodies or Turkish courts, the application of the Law itself is practically limited to real and legal persons who are processing the PII of the persons residing in Turkey. Despite issues regarding the enforceability of sanctions against persons who are not in Turkey or do not have assets in Turkey, the content and structure of the DPL does make it clear that it is intended to establish and safeguard the data protection rights of all persons within Turkey whose personal data is being processed, regardless of the identity of the data processor. As a result, the DPL will apply to data controllers and data processors both inside and outside of Turkey that are processing the personal data of the Turkish residents.

This approach is also confirmed by the Regulation on Registry, which refers to data controllers that are based outside of Turkey. According to this Regulation, data controllers that are based outside of Turkey must be registered with the Registry established by the DPA and appoint a representative (either a legal entity based in Turkey or a Turkish citizen).

10 Covered uses of PII

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

The DPL also provides a very wide scope definition for the processing of PII. As per the relevant provision, processing of personal data is defined as 'all operations performed on personal data, whether completely or partially through automated means or – on the condition that it is a part of a data recording system – through non-automated means, such as collection, recording, structuring, storage, re-structuring, disclosure, transfer, retrieval, making available, categorisation or restriction'.

The DPL also distinguishes between data controllers, who determine the purposes and methods of data processing, and data processors that process data based on the authorisation provided by the data controllers.

Data controllers and data processors have different duties under the DPL. The most important of the obligations of data controllers are the requirements to notify and inform data subjects of the processing of their data and to obtain their consents where necessary under the DPL, to implement all kinds of technical and administrative measures in order to maintain a security level that would prevent unlawful processing of and unauthorised access to personal data while also safeguarding personal data, and to register with the Registry. The data controller and the data processor that processes data on behalf of the data controller are jointly responsible for the adoption of these technical and administrative measures.

Legitimate processing of PII

11 Legitimate processing – grounds

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

Pursuant to the DPL, in principle the personal data can be processed with the explicit and informed consent of the data subject. However, the DPL itself also provides additional conditions where this requirement of obtaining explicit and informed consent will not be required, which are set forth below:

- processing is clearly mandated by laws;
- for a person who is unable to express their explicit consent owing to a situation of impossibility, processing is required for the safeguarding of their or a third person's life or physical wellbeing;
- processing is necessary for and directly related to the formation or execution of an agreement to which the data subject is a party;
- processing is mandatory for the data controller to satisfy his or her legal obligation;
- the data to be processed has been made public by the data subject;
- processing is mandatory for the establishment, use or protection of a right; or
- on the condition that it does not harm the data subject's fundamental rights and freedoms, the processing is mandatory for the legitimate interests of the data controller.

Although the DPL specifies the explicit consent of the data subject as the main principle for processing personal data, the DPA states that if it is possible to process the personal data based on any of the additional conditions set forth above, the data controller should process the data based on the additional condition and should not obtain explicit consent.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Yes, the DPL provides more stringent rules for the processing of personal data of a sensitive nature. Personal data of a sensitive nature is defined exhaustively as data relating to 'race, ethnicity, political views, philosophical belief, religious denomination or other beliefs, clothing and attire, membership in associations, charities or trade unions, health, sex life, convictions, security measures, biometric and genetic data'.

While the general principle for the processing of such data remains the explicit consent of the data subject, the situations of exception are a lot narrower compared to normal PII. With regard to personal data of a sensitive nature other than health and sex life data, processing without consent is allowed when such processing is clearly mandated by law. For health and sex life data, the only exception is data processed by persons or authorised institutes bound by the duty of confidentiality for the purpose of the protection of public health, the provision of medical, diagnostic and treatment services and the planning, management and financing of healthcare services.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The DPL does include a duty of notification that requires data controllers to notify the data subjects as to the use of their data. This notification must be made at the time that the personal data is obtained and must include the following information:

- the identity of the data controller and, if applicable, its representative;
- the purposes of processing;
- to whom the processed data may be transferred and for which purposes they may be transferred;
- the method and legal grounds for the data collection; and
- information about the other rights of the data subject.

14 Exemption from notification

When is notice not required?

The conditions for exemption from the obligation of notification are when:

- the processing is required for the prevention or investigation of a crime;
- the data being processed has been made public by the data subject;
- the processing is required for disciplinary investigations or procedures by authorised public bodies and institutions, or by professional organisations with public institution status and for the inspections carried out by such parties in accordance with their statutory purview; or
- the processing is required to protect the state's economic and financial interests with regard to the issues of budget, taxation and financial issue.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

As the DPL upholds the central principle that data processing should be based on consent and that processing should be in accordance with the law and the principle of honesty, it can be said that by the very nature of the centrality of explicit consent, the data subjects are afforded a degree of control over their information. The exceptions to the requirement of consent do provide derogations from this notion of control; however, as will be further discussed in questions 37–40, data subjects have been granted substantial rights to ensure that their data is being processed in accordance with the original purpose of the processing of their PII.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

One of the main principles of the DPL is that the processed personal data be accurate and – when necessary – up to date. While there has not been any further guidance as to the standards of accuracy and quality of the personal data, it is expected that these principles will be further clarified by the Turkish DPA through the drafting and publication of ancillary regulatory measures.

The DPL also grants data subjects the right to demand that any personal data relating to them that has been processed in an incorrect or incomplete manner be rectified.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The DPL itself does not state set and definite time limits for how long personal data may be held. However, article 7 of the DPL introduces a general principle stating that, once the grounds of processing of personal data no longer exist, the data controller is under the obligation to either delete, destroy or anonymise the personal data. While these processes may be applied upon the request of the data subject, the DPL also states that the data controller itself should also apply these processes through its own determination.

With regard to the amount of PII, as long as all processed PII is being held and processed lawfully, the DPL does not enforce any restrictions as to the amount or volume of data.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Article 4 of the DPL provides the fundamental principles of data processing in Turkey; one of which is that processing must be in connection with, limited to and proportional to the stated purposes of processing. Therefore, as per the DPL, processing of personal data must be limited to either the purpose for which explicit consent was provided or to the scope of the exception to obtaining explicit consent upon which the processing can be based.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

As stated above, due to the adoption of the finality principle requiring processing to be connected, limited and proportional to the stated purpose of processing, the DPL does not allow for using collected personal data for new purposes that are not covered by the obtained explicit consent or the specific grounds of exception that have been used for processing. Furthermore, the Communiqué on Procedures and Principles regarding the Obligation to Notify states that the data controller must comply with the notification obligation before starting the data processing activity if the purpose of the data processing is changed.

Security

20 Security obligations

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

The DPL imposes general security obligations on data controllers to ensure that personal data is not processed unlawfully, accessed without authorisation and is safeguarded. The relevant provision stipulates a general obligation of ensuring that all technical and administrative precautions are taken by the data controller in order to ensure that such protection is provided. Furthermore, as per the provision of the DPL that establishes the conditions of processing personal data of a sensitive nature, such processing is conditioned upon implementing the sufficient measures that have been determined by the Turkish DPA.

Since the DPL itself does not provide detailed explanations as to the content of these precautions, the DPA issued the Guidelines on Personal Data Security (Technical and Administrative Measures) in January 2018 and the Decision Regarding the Adequate Measures to be Taken by Data Controllers in Processing of Personal Data of Sensitive Nature on 7 March 2018 (Decision on Adequate Measures).

Finally, pursuant to the DPL, data controllers are also under the obligation to conduct the required audits in order to ensure that they are adhering to the security provisions of the DPL. In the situation that a data controller utilises a third-party data processor to process PII on their behalf, the data controller will remain jointly liable with regard to ensuring that safety precautions are taken to ensure the protection of the PII.

21 Notification of data breach

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 DPL requires for any access to data by third parties through unlawful means to be notified by the data controller to both the data subject and the Turkish DPA. The DPL also stipulates that, should the Turkish DPA deem it necessary, it may publish such notified breaches either on its own website or through other appropriate means.

Currently there are no further clarifications regarding this duty of notification, particularly with regard to any set time limit within which to notify such breaches to the data subjects and the DPA. The relevant provision only states that such notifications must be made 'within the shortest possible time'. Thus, it is expected that the Turkish DPA will issue ancillary regulations to clarify this issue.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The DPL and other sector-specific ancillary regulations do not require the appointment of a data protection officer. However, the Regulation on Registry requires data controllers that are based in Turkey to appoint a contact person, who will be responsible for communication of the requests of data subjects to the data controller and will be the contact person for the Turkish DPA. Similarly, data controllers that are based outside of Turkey are required to appoint a representative, who will be the contact person for the Turkish DPA and the Turkish Data Protection Board, for responding to the queries addressed to the data controller and conveying the responses of the data controller to data subjects and taking necessary actions concerning registration procedures to the Registry.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The DPL does not contain a provision regarding a general obligation to maintain internal records or establish internal processes or documentation. However, the Regulation on Deletion, Destruction and Anonymisation of Personal Data requires all data controllers to maintain data inventories, and data controllers that are responsible for enrolling in the Registry to maintain a personal data retention and destruction policy. Furthermore, the Decision on Adequate Measures requires data controllers that process personal data of a sensitive nature to adopt and maintain a systematic and sustainable policy and procedure for the safety of personal data of a sensitive nature.

On the other hand, for the time being, none of this legislation sets forth any obligation for data processors to maintain any internal records or establish internal processes or documentation. However, for evidentiary purposes, processors and controllers should maintain records to prove that they have acted in compliance with the DPL in case of an audit or conflict.

With regard to the electronic communication sector, the ECL and ancillary regulatory measures require licensed operators within the electronic communication sector to maintain certain records relating to completed and attempted electronic communications. Furthermore, licensed operators are also under an obligation to maintain records that document access made to personal data and other related systems for a period of two years.

24 New processing regulations

Are there any obligations in relation to new processing operations?

There is no explicit obligation in relation to new processing operations such as requirements to apply a privacy-by-design approach or carry out a privacy impact assessment. However, the DPL regulates the general principles of the processing of personal data, and within this scope all processing activities must comply with the laws and the rule of bona fide; be accurate and up to date; be for specific, legitimate and explicit purposes; be in connection with, limited to and proportional to the purposes of processing; and personal data must be kept only for the period required for the processing purposes or as regulated under the relevant legislation.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

As per the DPL, both real and legal persons processing PII must be registered on the Registry. Depending on the provision of the DPL that enables the Turkish DPA to introduce exemptions for registration to the Registry based on such considerations as the quality, amount and grounds of the processing, the Turkish DPA issued a principle decision dated 2 April 2018 that specifies the exemptions of the registration. According to the relevant decision of the Turkish DPA, data controllers that process personal data only in non-automatic ways, within the part of a data recording system; associations, foundations and unions that process personal data of their employees, members and donors only within the scope of the relevant legislation and limited with the purposes of their activities; notaries; political parties, lawyers, public accountants and sworn-in public accountants are exempted from registration.

Furthermore, article 28(2) of the DPL also introduces a more general exemption from the obligation to register for instances of

processing where, on the condition that it remains in accordance and proportional to the purpose and principles of the DPL:

- the processing is required for the prevention or investigation of a crime;
- the data being processed has been made public by the data subject;
- the processing is required for disciplinary investigations or procedures by authorised public bodies and institutions or by professional organisations with public institution status and for the inspections carried out by such parties in accordance with their statutory purview; or
- the processing is required to protect the state's economic and financial interests with regard to the issues of budget, taxation and financial issue.

These general exemptions are also repeated under article 15 of the Regulation on Registry.

26 Formalities

What are the formalities for registration?

The DPL establishes the general principles relating to registration with the Registry. As per said principles, the data controller's application for registration must include the following information:

- the identity and address of the data controller and, if applicable, his or her representative;
- the purpose of processing of the personal data;
- the data subject groups and explanations relating to the data categories belonging to these persons;
- recipients or recipient groups to whom the data may be transferred;
- the precautions taken with regard to the security of personal data; and
- the maximum time period required for the process of processing.

In order to detail the registration process, the Turkish DPA issued the Regulation on Registry on 30 December 2017. As per this Regulation, for registration to the Data Controllers Registry Information System (VERBİS), data controllers must prepare data inventories as well as data retention and destruction policies. Furthermore, data controllers that are based in Turkey must appoint a contact person and data controllers that are based outside of Turkey must appoint a data controller's representative.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

In the situation that a data controller fails to register for the Registry or fails to maintain their registration with up-to-date information, said controller can be sanctioned with an administrative fine ranging from 20,000 to 1 million liras.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Currently the DPL or the Regulation on Registry do not provide any specific grounds on which the Turkish DPA could refuse to allow an entry on the Registry. In order to register with the Registry, an individual or a legal entity must be a data controller, and thus the Turkish DPA can refuse to allow an entry only if the applicant is not a data controller or if the data controller does not provide all of the required information for registry.

29 Public access

Is the register publicly available? How can it be accessed?

Yes, the DPL and the Regulation on Registry set forth that the Registry will be open to the public. According to the Regulation, the registration of data controllers will take place electronically based on VERBİS, which will be open to the public. Currently, the Turkish DPA is working on the technical aspects of VERBIS, and VERBIS is expected to be opened soon.

30 Effect of registration

Does an entry on the register have any specific legal effect?

No. Currently, the DPL or the Regulation on Registry do not explicitly attach any specific legal effect to entry on to the Registry.

31 Other transparency duties

Are there any other public transparency duties?

No, there are no other transparency duties.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The DPL has regulated all transfers from data controllers to third parties, without making any differentiation in terms of outsourced data processors. Therefore, there is no specific provision or exemption applicable to the transfers of PII to entities that provide outsourced processing services.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Other than adhering to the requirement of obtaining explicit consent from the data subject (in cases where there is no area of exception to obtaining such explicit consent), there are no further restrictions on the disclosure of PII to third parties within Turkey.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The general principle with regard to transfer of personal data outside of Turkey is that the explicit consent of the data subject is required. However, in the situation that one of the general exceptions of obtaining consent for personal data or for personal data of a sensitive nature exists, said personal data may be transferred outside of Turkey if the country of the recipient provides 'sufficient safeguards'. If the country where the recipient is located does not provide 'sufficient safeguards', the personal data may only be transferred if the data controllers in Turkey and in the related foreign country undertake to ensure sufficient protection in writing and the Turkish DPA authorises such transfer. Currently, there is no list specifying the countries that provide sufficient safeguards; however, the Turkish DPA is expected to publish a decision in this regard soon.

A general restriction that applies to the transfer of personal data outside of Turkey regards considerations of national interest. Reserving the applicable provisions of international agreements, in the situation that the interests of Turkey or the data subject will be seriously harmed, said personal data may only be transferred abroad with the consent of the Turkish Data Protection Board.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

As stated above, in the situation that explicit consent for transfer has not been obtained and, instead, the data controller is to transfer personal data abroad based on one of the exceptions defined in the DPL, the country where the recipient is located must provide 'sufficient safeguards'. In the situation that the Turkish DPA has not determined said country to be on the list of 'countries providing sufficient safeguards', transfer of data abroad can only be completed if both data controllers provide written undertakings to ensure sufficient safeguards and if the Turkish DPA authorises the transfer.

However, this requirement of notification and authorisation is only required for a transfer abroad based on an exception to a recipient in a country not providing 'sufficient safeguards'. For all other transfers there are no general or specific obligations to notify the Turkish DPA or obtain authorisation for transfer.

36 Further transfer

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

Currently the DPL only explicitly covers the issue of the initial transfer abroad, with no explicit provisions detailing subsequent onward transfers. Consequently, it should be accepted that the provisions relating to transfer abroad apply equally to such further transfers, and the detailed explanations provided above should be taken into consideration.

Rights of individuals

37 Access

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

As per the DPL, individuals have been granted the right to access their personal information held by data controllers. In addition to the right to learn whether or not their personal data is being processed, individuals also have a right to know the purpose of the processing of their data and whether the current processing is in accordance with this purpose and the right to know to whom their data is being transferred, both domestically and abroad.

However, these rights of access can be limited in the following situations, on the condition that it remains in accordance and proportional to the purpose and principles of the DPL where:

- the processing is required for the prevention or investigation of a crime;
- the data being processed has been made public by the data subject;
- the processing is required for disciplinary investigations or procedures by authorised public bodies and institutions or by professional organisations with public institution status and for the inspections carried out by such parties in accordance with their statutory purview; and
- the processing is required to protect the state's economic and financial interests with regard to the issues of budget, taxation and financial issue.

38 Other rights

Do individuals have other substantive rights?

In addition to the rights explained in our response to question 37, the DPL has also granted individuals other substantive rights to exercise.

As per article 11 of the DPL, data subjects have the following substantive rights with regard to the processing of their personal data:

- the right to ask for rectification of any data that has been processed in an incomplete or wrong manner;
- the right to request the deletion or destruction of their personal data where the grounds of processing of the personal data no longer exist;
- the right to have their requests of rectification or deletion notified to any third parties to whom their personal data has been transferred; and
- the right to object to a decision made against them based solely on analysis of personal data through automated processing.

39 Compensation

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 DPL clearly states that individuals have the right to compensation in the situation that the unlawful processing of their personal data has caused them to suffer damage. Therefore, in the situation that a breach of the DPL causes a person damage, she or he will be able to file a compensation action seeking monetary damages against the offending data controller.

Under Turkish law, compensation claims can be filed for both pecuniary and non-pecuniary damages for pain and suffering. However, it should be noted that in Turkish practice, non-pecuniary damages are rarely granted in situations where there has not been actual damage.

40 Enforcement

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

The DPL provides that data subjects must first apply to the relevant data controller with any complaints that they have regarding the exercise of their data protection rights. Should such an application not be answered in 30 days, rejected or should the data subject be unsatisfied with the response, the data subject will then have the right to refer the complaint to the Turkish DPA.

In addition to the complaint procedure that can ultimately be referred to the Turkish DPA for resolution, data subjects may exercise their rights relating to unlawful access or transfer of their personal data through the judicial system.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Other than the exemptions and derogations explained above in questions 5, 14 and 25, there are no further exemptions or limitations on the application of the provisions of the DPL.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

As the Turkish DPA is an administrative body, as per the general principles of Turkish administrative law, the decisions and actions of the body can be appealed through administrative courts.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

While there are no general legislative or regulatory measures relating to the use of cookies, the ECL does contain rules on the use of cookies that are specific to operators that have been licensed in accordance with the relevant electronic communication legislation. As per said specific rules, licensed operators may only store information on the devices of their customers, or reach stored information on these devices if they have obtained informed and explicit consent.

However, it should be noted that for any use of cookies that will involve PII, the relevant safeguards and measures of the DPL will also apply.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

The general rules on marketing through any means of electronic communication have been defined in the E-Commerce Law. As per the E-Commerce Law, the general rule for sending any form of electronic commercial communication is that the consent of the recipient is obtained in advance. Such consent may be obtained either in writing or by using any form of electronic communication tool. Additionally, such recipients must always be provided the opportunity to opt out of receiving such communication at any time and without having to specify any reason.

Certain electronic communications can be sent without first obtaining the explicit consent of the recipient. These communications are either communications with the purpose of providing information on the changes, use and repair of the provided goods or services sent to recipients who have readily provided their contact information, or if the electronic communications are being sent to a tradesmen or merchant. However, such recipients should also be provided with the aforementioned chance to opt out of receiving such electronic communications.

Furthermore, the content of the electronic commercial communication must be in line with the consent obtained from the recipient.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

There are currently no rules or regulatory guidance specifically relating to the use of cloud computing services. However, the Information and Communication Technologies Authority has been working on a draft guidance document relating to standards that should be adopted in this area.

Furthermore, in accordance with the aforementioned provisions of the DPL regarding the transfer of data to third parties and transfer of data abroad, it should be noted that the requirements relating to such transfers can also be applied to situations where cloud computing services are obtained from companies with servers abroad.

United Kingdom

Aaron P Simpson and James Henderson
Hunton Andrews Kurth LLP

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The primary legal instruments include the UK's Data Protection Act 2018 (DPA) and the EU's General Data Protection Regulation 2016/679 (GDPR) on the protection of individuals with regard to the processing of PII and the free movement of data. The UK is a signatory to Treaty 108 of the Council of Europe. The UK has no national constitutional privacy provisions but is bound by the EU Charter of Fundamental Rights.

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 two-year process of leaving the EU. Although the process of 'Brexit' is under way, it remains unclear what future trading arrangements will be agreed between the UK and the EU. If the UK seeks to remain part of the EEA, it will need to continue to adopt EU laws, including the GDPR. If the UK is outside the EU or EEA, it is likely to seek adequacy status to enable data flows between the UK and the EEA. This will require data protection laws that are essentially equivalent to EU data protection laws (ie, GDPR) but may be complicated by the UK's Investigatory Powers Act 2016, which permits the type of bulk surveillance practices that the Court of Justice of the European Union believes fail to respect data protection principles. Further, non-EU controllers or processors that process the personal data of EU data subjects in the context of offering goods or services to them or monitoring their behaviour will be subject to the GDPR in any event.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The DPA and the 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.

3 Legal obligations of data protection authority

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

The ICO participates in the 'one-stop shop' under the GDPR, under which organisations with a main establishment in the EU may primarily be regulated by the supervisory authority of the jurisdiction in which the main establishment is located (lead supervisory authority). The DPA and the GDPR confer on the ICO powers to participate in the GDPR's one-stop shop, cooperate with other concerned supervisory authorities, to request from and provide mutual assistance to other concerned supervisory authorities, and to conduct joint operations, including joint investigations and joint enforcement actions with other concerned supervisory authorities. The status of the ICO's participation in the EU's one-stop shop once the UK has left the EU is currently not clear.

The DPA also requires the ICO, in relation to third countries and international organisations, to take steps to develop cooperation mechanisms to facilitate the effective enforcement of legislation relating to the protection of personal data, to provide international mutual assistance in the enforcement of legislation for the protection of personal data, to engage relevant stakeholders in discussion and activities, and to promote the exchange and documentation of legislation and practice for the protection of personal data.

4 Breaches of data protection

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

The ICO has a number of 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 €20 million or 4 per cent of annual worldwide turnover, depending on the nature of the violation of the DPA and GDPR.

A number of breaches may lead to criminal penalties. The following may constitute criminal offences:

- making a false statement in relation to an information notice validly served by the ICO;
- destroying, concealing, blocking or falsifying information with the intention of preventing the ICO from viewing or being provided with the information;
- unlawfully obtaining PII;
- knowingly or recklessly re-identifying PII that is de-identified without the consent of the data controller responsible for that PII;
- altering PII so as to prevent disclosure of the information in response to a data subject rights request; and
- obstructing 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.

Scope

5 Exempt sectors and institutions

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 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' activities.

The GDPR and the DPA apply to private and public sector bodies, including law enforcement agencies and intelligence services.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Electronic marketing is specifically regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (as amended), although the GDPR and the DPA often apply to the same activities, to the extent that they involve the processing of PII. Interception and state surveillance are covered by the Investigatory Powers Act 2016. The interception of business communications is regulated by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

7 Other laws

Identify 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 PII. Laws on defamation, copyright and computer misuse also affect data protection. However, there is no specific data protection sectoral legislation. The UK 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 requires the ICO to draw up and publish codes of practice that relate to data sharing, direct marketing, age-appropriate design and data protection and journalism.

8 PII formats

What forms of PII are covered by the law?

The GDPR and the DPA cover PII held in electronic form plus such information held in structured files, called 'relevant filing systems'. In order 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.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Organisations that are data controllers or data processors fall within the scope of the law if they are established in the UK and process PII in the context of that establishment, or if they are not established in the EU but offer goods or services to individuals located in the UK, or monitor their behaviour.

A data controller or data processor is 'established' in the UK if it is resident in the UK, 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 UK.

Data controllers established outside the EU that are subject to the GDPR and the DPA must nominate a representative in the UK.

10 Covered uses of PII

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

The GDPR and the DPA are applicable to data controllers (ie, those that decide the purposes and the means of the data processing) and data processors (who merely process PII on behalf of data controllers).

Legitimate processing of PII

11 Legitimate processing – grounds

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

The GDPR requires data controllers to rely on a legal ground set forth in the GDPR for all processing of PII. Additional conditions must also be satisfied when processing sensitive PII (see question 12).

The grounds for processing non-sensitive PII are:

- consent of the individual;
- performance of a contract to which the individual is party;
- compliance with a legal obligation, other than a contractual obligation (a legal obligation arising under the laws of a non-EU 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 PII is disclosed), unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Distinct grounds for legitimate processing apply to the processing of sensitive PII. 'Sensitive' PII is defined as PII relating to:

- 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 for the purpose of uniquely identifying 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.

The GDPR sets forth a number of grounds that may be relied upon for the processing of sensitive PII, 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);
- the processing relates to PII which is manifestly made public by the data subject;
- the exercise of public functions;
- processing in connection with legal proceedings, legal advice or in order to exercise legal rights; or
- processing for medical purposes.

In addition to the grounds set forth in the GDPR, the DPA sets forth a number of additional grounds 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 PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? 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 PII 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 PII;
- the fact that the data controller intends to transfer the PII 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 the means by which individuals may obtain a copy of them;
- the period for which PII 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 an EU data protection supervisory authority;
- whether the provision of PII 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 PII and of the consequences of failure to provide such PII; 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.

Notice must be provided at the time the PII is collected from the data subject. When PII is obtained from a source other than the individual concerned, then the data controller must also inform individuals of the source from which the PII originated.

14 Exemption from notification

When is notice not required?

Where PII 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 require disproportionate effort (in which case the data controller shall take appropriate measures to protect data subjects, including making the relevant information publicly available);
- obtaining or disclosure of the PII is required by EU law to which the data controller is subject; or
- where the PII is subject to an obligation of professional secrecy under UK or EU law.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Individuals have a number of rights in relation to PII held by data controllers:
- to obtain confirmation of whether the data controller processes PII about the individual and to obtain a copy of that PII;
- to rectify PII that is inaccurate;
- to have PII erased in certain circumstances; for example, when the PII is no longer necessary for the purposes for which it was collected by the data controller;
- to restrict the processing of PII;
- to obtain a copy of PII in a structured, commonly used and machine-readable format, and to transmit that PII to a third-party data controller without hindrance, to the extent that it is technically feasible;
- to object to the processing of PII in certain circumstances; and
- not to be subject to decisions based solely on the automated processing of PII, except in particular circumstances.

Data processors are not required to comply with data subject rights requests, but are required to provide assistance to data controllers on whose behalf they process PII to respond to any such requests.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The data controller must ensure that PII is relevant, accurate and, where necessary, kept up to date in relation to the purpose for which it is held.

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The data controller must ensure that PII is adequate, relevant and not excessive in relation to the purpose for which it is held. This means that the data controller should not collect or process unnecessary or irrelevant PII. The DPA and GDPR do not impose any specified retention periods. PII may be held only for as long as is necessary for the purposes for which it is processed.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

PII 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 DPA.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

PII may not be processed for new purposes unless the further purposes are lawful (ie, based on a lawful ground; see question 11). 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, PII 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.

Security

20 Security obligations

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

The DPA and GDPR do not specify the types of security measures that data controllers and data processors must take in relation to PII. Instead, data controllers and data processors must have in place 'appropriate technical and organisational measures' to protect against 'unauthorised or unlawful processing of [PII] and against accidental loss or destruction of, or damage to, [PII]'. In addition, the GDPR provides

several examples of security measures that data controllers and data processors should consider implementing, including:

- the pseudonymisation and encryption of PII;
- 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 PII in a timely manner 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 PII in question and the harm that might result from its improper use, or from 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 PII, it must choose a data processor providing sufficient guarantees of security, take reasonable steps to ensure that these are delivered, require the processor to enter into a contract in writing under which the 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.

21 Notification of data breach

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 GDPR requires data controllers to notify the 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 promptly notify affected individuals of a breach 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 to affected individuals, but data processors must notify the relevant data controller of a data breach promptly.

In addition to notifying breaches to the ICO and to affected individuals, data controllers must also document data breaches and retain information relating to the facts of the breach, its effects and the remedial action taken.

Internal controls

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The GDPR requires data controllers and data processors to appoint a data protection officer if:

- the core activities of the data 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 data controller or processor consist of processing sensitive PII or PII relating to criminal offences and convictions on a large scale.

If appointed, the data protection officer is responsible for:

- informing and advising the data controller or processor and its employees of their obligations pursuant to data protection law;
- monitoring compliance with the GDPR, awareness raising, staff training and audits;
- providing advice with regard to data protection impact assessments;
- cooperating with the ICO and other EU data protection supervisory authorities; and
- acting as a contact point for the ICO on issues relating to processing PII.

Organisations may also elect to appoint a data protection officer voluntarily, although such an appointment will need to comply with the requirements of the GDPR.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Data controllers and data processors are required to retain internal records that describe the processing of PII 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 data protection officer;
- the purposes of the processing;
- the data subjects and categories of PII processed;
- the categories of recipients to whom PII has been or will be disclosed;
- a description of any transfers of PII to third countries and the safeguards relied upon;
- the envisaged time limits for erasure of the PII; 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 of each data controller on behalf of which the processor processes PII, and of the processor's representative and data protection officer;
- the categories of processing carried out on behalf of each data controller;
- a description of any transfers of PII to third countries and the safeguards relied upon; and
- a general description of the technical and organisational security measures implemented.

24 New processing regulations

Are there any obligations in relation to new processing operations?

Data controllers are required to carry out a data protection impact assessment in relation to any processing of PII that is likely to result in a high risk to the rights and freedoms of natural persons. In particular, a data protection impact assessment 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 PII or PII relating to criminal convictions or offences on a large scale; or
- systematic monitoring of a publicly accessible area on a large scale.

A data protection impact assessment must be carried out in relation to all high risk processing activities that meet the criteria above before the processing begins. The data protection impact assessment must include at least the following:

- a systematic description of the processing operations and the purposes of the processing;
- an assessment of the proportionality and necessity of the processing;
- an assessment of the risks to the rights and freedoms of affected individuals;
- information about the measures envisaged to address any risks to affected individuals.

The GDPR also 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 PII is processed in accordance with the GDPR, and to ensure that, by default, only PII that is necessary for each specific purpose is collected and processed. In addition, data controllers must ensure that by default PII is not made accessible to an indefinite number of persons without any intervention by the data subject.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

In the UK, data controllers are required to pay an annual registration fee to the 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 for the purposes of establishing or maintaining membership or support of that organisation; or
- the data controller only processes PII for one or more of these purposes:
  - staff administration;
  - advertising, marketing and public relations; or
  - accounts and records.

An entity that is a data processor only is not required to make this payment.

26 Formalities

What are the formalities for registration?

There is a three-tier fee structure in the UK. Data controllers must pay a fee according to the following criteria:

- if the data controller has a maximum turnover of £632,000 or no more than 10 members of staff, £40;
- if the data controller has a maximum turnover of £36 million or no more than 250 members of staff, £60; or
- in all other cases, £2,900.

The data controller must include in the fee application its name, address, contact details of the person who is completing the fee registration and contact details of the data controller's data protection officer if it is required to appoint one. Data processors are not required to pay the registration fee.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

PII must not be processed unless the data controller has paid the required fee.

If the data controller has not paid a fee when required to do so or has not paid the correct fee, it may be subject to a fixed monetary penalty of 150 per cent of the highest charge payable by a data controller (ie, £4,350). As previously noted, an entity that is a data processor only (and not a data controller) is not required to register or pay the fee.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The ICO has no power to refuse the application provided that it is made in the prescribed form and includes the applicable fee.

29 Public access

Is the register publicly available? How can it be accessed?

The fee register is publicly available, free of charge, from the ICO's website (https://ico.org.uk/esdwebpages/search).

A copy of the register on DVD may also be requested by sending an email to accessICOinformation@ico.org.uk.

30 Effect of registration

Does an entry on the register have any specific legal effect?

An entry on the register does not cause the data controller to be subject to obligations or liabilities to which it would not otherwise be subject.

31 Other transparency duties

Are there any other public transparency duties?

There are no additional public transparency duties.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Entities that provide outsourced processing services are typically 'data processors' under the DPA and the GDPR. Data processors are subject to direct legal obligations under the DPA and GDPR in respect of the PII that they process as outsourced service providers, but nevertheless data controllers are required to use only data processors that are capable of processing PII in accordance with the requirements of the DPA and the GDPR. The data controller must ensure that each processor it selects offers sufficient guarantees that the relevant PII will be held with appropriate security and takes steps to ensure that these guarantees are fulfilled. The data controller must also enter into a contract in writing with the processor under which the processor must be bound to:

- act only on the instructions of the data controller;
- ensure that persons that will process PII are subject to a confidentiality obligation;
- apply security controls and standards that meet those required by the 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 in relation to the obligations to notify personal data breaches and to carry out data protection impact assessments;
- at the choice of the data controller, return the PII to the data controller or delete the PII at the end of the relationship; 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.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

It is a criminal offence to knowingly or recklessly obtain or disclose PII without the consent of the data controller or procure the disclosure of PII to another party without the consent of the data controller. This prohibition is subject to a number of exceptions, such as where the action was taken for the purposes of preventing or detecting crime. The staff of the ICO are prohibited from disclosing PII obtained in the course of their functions other than in accord with those functions.

There are no other specific restrictions on the disclosure of PII, other than compliance with the general principles described earlier, and the cross-border restrictions as set out in question 34.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The transfer of PII outside the EEA is prohibited unless that country or territory ensures an adequate level of protection for the rights and freedoms of the individuals in relation to the processing of their PII.

Transfers are permitted where:

- the European Commission (Commission) has made a finding in relation to the adequacy of the country or territory;
- the Commission has made a finding in relation to the relevant transfers; or
- one or more of the derogations applies.

The derogations include:

- where the data controller has the individual's consent to the transfer;
- the transfer is necessary for a contract with the data subject;
- the transfer is necessary for legal proceedings;

Update and trends

On 29 March 2017, the UK government officially invoked article 50 of the Treaty of Lisbon, triggering the two-year process at the end of which the United Kingdom will leave the European Union. The move follows a UK referendum on EU membership held on 23 June 2016 where a narrow majority (approximately 52 per cent) voted in favour of leaving the bloc. The nature of the UK's relationship with the EU once it is no longer a member is currently the source of significant political friction. This has generated uncertainty over the future of a number of UK laws that have emanated from Brussels, including the GDPR.

The UK and EU will continue to rely on each other as major trade partners after Brexit, and the free movement of personal data will remain important in an increasingly information-rich age. This will depend on the EU deeming that the UK has adequate safeguards in place to ensure the protection of personal data. Although the UK has adopted the GDPR and the UK government has stated that it intends to retain the GDPR in UK law after the UK has left the EU, there is no guarantee that the UK will secure such a finding. The recently adopted Investigatory Powers Act 2016, which has been given the nickname 'the Snoopers' Charter' by the British media, permits bulk surveillance practices by UK authorities in certain circumstances. Such practices by US intelligence agencies contributed to the EU's invalidation of the Safe Harbor transfer mechanism in 2015. It remains unclear, therefore, whether the EU will deem that the UK provides an adequate level of data protection once the UK has left the EU.

- the transfer is necessary to protect the vital interest of the individual; and
- the terms of the transfer have been approved by the ICO.

Commission findings have been made in respect of the use of approved standard form model clauses for the export of PII and the adoption of a self-regulatory scheme in the US called the EU–US Privacy Shield, which replaced the Safe Harbor mechanism that was invalidated by the Court of Justice of the European Union in October 2015. In addition, entities within a single corporate group can enter into data transfer agreements known as binding corporate rules, which must be approved by the supervisory authorities in the relevant EU member states.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Transfer requires no specific notification to the ICO and no authorisation from the ICO.

36 Further transfer

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 taken into account in assessing whether adequate protection is provided in the receiving country. Onward transfers are covered in the Commission-approved model clauses, and in the Privacy Shield (which replaces the now invalid Safe Harbor framework).

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 Commission. It would be anticipated that the law of the recipient country would deal with the legitimacy of the onward transfer.

Rights of individuals

37 Access

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

Individuals have the right to request access to PII that relates to them. Within one month of receipt of a valid request, the data controller must supply a statement that it processes or does not process PII relating to that subject and, if it does so, a description of the PII, the purposes of the processing and recipients or categories of recipients of the PII, the relevant retention period for the PII, a description of the rights available to individuals under the GDPR and that the individual may complain to a supervisory authority and any information available to the controller as to the sources of the PII. The data controller must also provide a copy of the PII 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 where that would breach the privacy of the third party and may reject repeated identical requests, or charge a reasonable fee taking into account the administrative costs of providing the information.

In some cases the data controller may withhold PII to protect the individual; for example, where health data is involved, or to protect other important specified public interests such as the prevention of crime. All such exceptions are specifically delineated in the law.

38 Other rights

Do individuals have other substantive rights?

Individuals have the following further rights:

- to rectify PII that is inaccurate;
- to have PII erased in certain circumstances; for example, when the PII is no longer necessary for the purposes for which it was collected by the data controller;
- to restrict the processing of PII;
- to obtain a copy of PII in a structured, commonly used and machine-readable format, and to transmit that PII to a third-party data controller without hindrance, to the extent that it is technically feasible;
- to object to the processing of PII in certain circumstances; and
- not to be subject to decisions based solely on the automated processing of PII, except in particular circumstances.

39 Compensation

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 DPA indicates that 'non-material' damage includes 'distress'.

40 Enforcement

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 the rights described in questions 37–39.

The ICO has no power to order the payment of compensation to individuals. Therefore, an individual who seeks compensation must take an action to the courts. All the other rights of individuals can be enforced by the ICO using the powers described in question 2.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The DPA, in accordance with the derogations permitted by the GDPR, provides three types of exemptions:

- exemptions from the obligations that limit the disclosure of PII;
- exemptions from the obligations to provide notice of uses of PII; and
- exemptions from the rights of access.

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 PII is made publicly available under other provisions.

Specific exemptions apply to allow the retention and use of PII for the purposes of research.

All exemptions are limited in scope and most apply only on a case-by-case basis.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Data controllers may appeal orders of the ICO to the General Regulatory Chamber (First-tier Tribunal). Appeals must be made within 28 days of the ICO notice and must state the full reasons and grounds for the appeal (ie, that the order is not in accordance with the law or the ICO should have exercised its discretion differently).

Appeals against decisions of the General Regulatory Chamber (First-tier Tribunal) can be made (on points of law only) to the Administrative Appeals Chamber of the Upper Tribunal, appeals from which may be made to the Court of Appeal.

Specific data processing

43 Internet use

Describe 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 consent. Consent must be validly obtained in accordance with the requirements of the GDPR. 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.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

It is unlawful to send unsolicited electronic marketing (ie, via technologies such as SMS, fax or email) unless the consent of the recipient has been obtained. 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 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 and has not yet opted out. Any consent obtained must comply with the GDPR's consent requirements.

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. Any individuals may apply to have their telephone number listed in this directory; a separate provision covers corporate entities.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific rules or legislation that govern the processing of PII through cloud computing, and such processing must be compliant with the DPA. The 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 the DPA and the use of cloud providers from outside the UK.

HUNTON ANDREWS KURTH

Aaron P Simpson **asimpson@HuntonAK.com**

30 St Mary Axe
London EC3A 8EP
United Kingdom

Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.HuntonAK.com

United States

Lisa J Sotto and Aaron P Simpson
Hunton Andrews Kurth LLP

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The US legislative framework for the protection of PII resembles a patchwork quilt. Unlike other jurisdictions, the US does not have a single dedicated data protection law, but instead regulates privacy primarily by industry, on a sector-by-sector basis. There are numerous sources of privacy law in the US, 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.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no single regulatory authority dedicated to overseeing data protection law in the US. 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 pursuant to 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 US. 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 the FTC 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 is able to fine businesses that have violated a consent order.

At the state level, attorneys general also have the ability to bring enforcement actions for unfair or deceptive trade practices, or to enforce violations of specific state privacy laws. Some state privacy laws allow affected individuals to bring lawsuits to enforce violations of the law.

3 Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with 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 a multistate task force 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.

4 Breaches of data protection

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 (ECPA) (which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act) or the Computer Fraud and Abuse Act (CFAA) can lead to criminal sanctions and civil liability. In addition, 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 DOJ may pursue criminal sanctions.

Scope

5 Exempt sectors and institutions

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 US. 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 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.

6 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Interception of communications is regulated primarily at the federal level by the ECPA, which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act. The federal CFAA 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.

7 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

In addition to the laws set forth above, there are numerous other federal and state laws that address privacy issues, including state information security laws and laws that apply to:

- consumer report information: the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act of 2003 (FACTA);
- children's information: the Children's Online Privacy Protection Act (COPPA);
- driver's information: the Driver's Privacy Protection Act of 1994;
- video rental records: the Video Privacy Protection Act; and
- federal government activities: the 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, which becomes effective on 1 January 2020. The Act applies to any for-profit business that:

- does business in California;
- collects consumers' personal information (or on behalf of which 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 50,000 or more consumers, households or devices.

The California Consumer Privacy Act defines 'personal information' broadly and contains provisions granting California consumers certain rights with respect to their personal information.

8 PII formats

What forms of PII are covered by the law?

The US does not have a dedicated data protection law. Thus, the definition of PII varies depending on the underlying law or regulation. In the state security breach notification law context, for example, the definition of PII 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 PII under the data breach notification laws to include such elements as medical information, insurance information, biometrics, email addresses and passwords to online accounts. In other contexts, such as FTC enforcement actions, GLB or HIPAA, the definition of PII is much broader. Although certain laws apply only to electronic PII, many cover PII in any medium, including hard copy records.

The California Consumer Privacy Act contains a broad definition of PII that includes any 'information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household'.

9 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

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 US.

10 Covered uses of PII

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

Generally, US privacy laws apply to all processing of PII. There are no formal designations of 'controllers' and 'processors' under US law as there are in the laws of other jurisdictions. There are, however, 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 PII 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.

Legitimate processing of PII

11 Legitimate processing – grounds

Does the law require that the holding of PII 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 retention of PII to certain specified grounds. There are, however, laws that may indirectly affect an organisation's ability to retain PII. 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 US, the organisation must provide a privacy notice detailing the PII the company collects and how it is used. If the organisation uses the PII in materially different ways than those set forth 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.

12 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Since the US 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, such as:

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 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 US, 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
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
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 California Consumer Privacy Act 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.

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 must 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 (SSN) laws
Numerous state laws impose obligations with respect to the processing of 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).

A number of state laws also impose restrictions targeting specific SSN uses.

Data handling responsibilities of owners of PII

13 Notification

Does the law require owners of PII to notify individuals whose PII they hold? 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's 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 PII collected through the website;
- the categories of third-party persons or entities with whom the operator may share the PII;
- the process an individual must follow to review and request changes to any of his or her PII 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 PII online over time and across third-party websites or online services, if the operator engages in such collection;
- whether third parties collect PII 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.

In addition to the requirements of the California Online Privacy Protection Act, the California Consumer Privacy Act requires businesses to provide notice to consumers of their rights under the Act (eg, the right to opt out of the sale of personal information), a list of the categories of personal information collected about consumers in the preceding 12 months and, where applicable, that the business sells or discloses their personal information. If the business sells consumers' personal information or discloses it to third parties for a business purpose, the notice also must include lists of the categories of personal information sold and disclosed about consumers, respectively. Businesses must separately provide a clear and conspicuous link on their website that says 'Do not sell my personal information' and provide consumers a mechanism to opt out of the sale of their personal information, a decision the business must respect. Companies must update their notices at least once every 12 months.

Delaware and Nevada have also enacted laws that require operators of commercial internet services to provide similar information to their users when collecting PII online. In addition to the California, Delaware and Nevada laws, there are other federal laws that require a privacy notice to be provided in certain circumstances, such as:

COPPA
Pursuant to the FTC's Children's Online Privacy Protection Rule, implemented pursuant to 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 prior to collecting, using or disclosing personal information from children.

FCRA and FACTA

The FCRA, as amended by 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, prescreened offers of credit or insurance, information sharing with affiliates, and adverse actions taken on the basis of a consumer report.

GLB

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 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 GLB privacy notice rule-making authority from the financial regulatory agencies to the CFPB. The CFPB then restated the GLB implementing regulations, including those pertaining to the model form, in Regulation P.

HIPAA

The Privacy Rule promulgated pursuant to 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 PHI;
- the individual's rights with respect to the PHI and how those rights may be exercised;
- a list of the covered entity's statutorily prescribed duties with respect to the PHI; and
- contact information for the individual at the covered entity responsible for addressing complaints regarding the handling of PHI.

14 Exemption from notification

When is notice not required?

Outside of the specifically regulated contexts discussed above, a privacy notice in the US must only be provided in the context of collecting personal information from consumers online. There is no requirement of general application that imposes an obligation on unregulated organisations to provide a privacy notice regarding its offline activities with respect to personal information. There is also no obligation to provide a general privacy notice in the employment context.

15 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

In the regulated contexts discussed above, individuals are provided with limited choices regarding the use of their information. The choices are dependent upon the underlying law. Under GLB, for example, customers and consumers have a legal right to opt out of having their non-public personal information shared by a financial institution with third parties (outside an enumerated exception). Similarly, under the FCRA, as amended by FACTA, individuals have a right to opt out of having certain consumer report information shared by a consumer reporting agency with an affiliate, in addition to another opt-out opportunity prior to any use of a broader set of consumer report information by an affiliate for marketing reasons. Federal telemarketing laws and the CAN-SPAM Act give individuals the right to opt out of receiving certain types of communications, as do similar state laws.

In addition, California's Shine the Light Law requires companies that collect personal information from residents of California generally to 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 preceding calendar year or, alternatively, to give the individuals the right to opt out of such third-party sharing. This right is expanded in the California Consumer Privacy Act, which provides that, upon request from a California consumer, an organisation must disclose:

- the categories and specific pieces of personal information the business has collected about the consumer;
- the categories of sources from which the personal information is collected;
- the business or commercial purposes for collecting or selling personal information; and
- the categories of third parties with whom the business shares personal information.

The California Consumer Privacy Act also provides consumers with the right to opt out of the sale of their personal information.

As the primary regulator of privacy issues in the US, the FTC periodically issues guidance on pressing issues. In the FTC's 2012 report entitled 'Protecting Consumer Privacy in an Era of Rapid Change', the FTC set forth guidance indicating that organisations should provide consumers with choices with regard to uses of personal information that are inconsistent with the context of the interaction through which the organisation obtained the personal information. In circumstances where the use of the information is consistent with the context of the transaction, the FTC indicated that offering such choices is not necessary.

16 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

There is no law of general application in the US that imposes standards related to the quality, currency and accuracy of PII. 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, pursuant to the HIPAA Security Rule, covered entities must ensure, among other things, the integrity of electronic protected health information (ePHI).

17 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

US privacy laws generally do not impose direct restrictions on an organisation's retention of personal information. There are, however, thousands of records retention laws at the federal and state level that impose specific obligations on how long an organisation may (or must) retain records, many of which cover records that contain personal information.

18 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

US privacy laws have not specifically adopted the finality principle. 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 set forth in the notice, it is likely that such a practice would be considered a deceptive trade practice under federal and state consumer protection laws.

19 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

In the US, organisations must use the personal information they collect in a manner that is consistent with the uses set forth in the privacy notice. To the extent an organisation would like to use previously collected personal information for a materially different purpose, 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 pursuant to COPPA), failure to handle the PII as described pursuant to such notice also may constitute a violation of the statute.

Security

20 Security obligations

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

Similar to privacy regulation, there is no comprehensive federal information security law in the US. Accordingly, the security obligations that are imposed on data owners and entities that process PII on their behalf depend on the regulatory context. These security obligations include:

GLB

The Safeguards Rule implemented pursuant to GLB 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. Although the Safeguards Rule is not prescriptive in nature, 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.

HIPAA

The Security Rule implemented pursuant to HIPAA, which applies to 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 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. In addition, 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 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. In addition, 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. 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 with respect to the processing of 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).

A number of 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 Payment Card Industry Data Security Standard (PCI DSS) applies to all entities that process credit or debit cards. It obligates covered entities to comply with prescriptive information security requirements, which include:

- installing and maintaining a firewall configuration to protect cardholder data;
- encrypting transmission of cardholder data across public networks;
- protecting systems against malware and regularly updating antivirus 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.

In addition, 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.

21 Notification of data breach

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:

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, the laws of 23 states 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, a number of jurisdictions do not employ such a harm threshold and require notification of any incident that meets their definition of a breach.

Federal Interagency Guidance

Several federal banking regulators issued the Interagency Guidance on Response Programs for Unauthorised Access to Customer Information and Customer Notice. 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 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. In addition, the Interagency Guidance contains two 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.

HITECH Act

The Health Information Technology for Economic and Clinical Health Act's (HITECH Act) information security breach provisions 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 HHS 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 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

22 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

No, the appointment of a data protection officer is not mandatory under the privacy rules of general application. Many organisations in the US 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, HIPAA requires the appointment of a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. In addition, several federal and state laws require that a chief information security officer or an equivalent be appointed. These laws include GLB, HIPAA and the NYDFS Cybersecurity Regulations.

23 Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

There are no legal requirements of general application that obligate owners of PII to maintain internal records or establish internal processes or documentation. As discussed in question 20, there are several statutory frameworks in the US that require organisations to develop an information security programme, which typically must contain internal processes and documentation. These include requirements imposed by GLB, HIPAA and state information security laws.

24 New processing regulations

Are there any obligations in relation to new processing operations?

There are no legal obligations in relation to new processing operations, such as to apply a privacy-by-design approach or carry out privacy impact assessments. The FTC 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.

Registration and notification

25 Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There are no registration requirements for data processing activities in the US.

26 Formalities

What are the formalities for registration?

There are no registration requirements for data processing activities in the US.

27 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There are no registration requirements for data processing activities in the US.

28 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

There are no registration requirements for data processing activities in the US.

29 Public access

Is the register publicly available? How can it be accessed?

There are no registration requirements for data processing activities in the US.

30 Effect of registration

Does an entry on the register have any specific legal effect?

There are no registration requirements for data processing activities in the US.

31 Other transparency duties

Are there any other public transparency duties?

See the response to question 13 regarding notification of individuals.

Transfer and disclosure of PII

32 Transfer of PII

How does the law regulate the transfer of PII to 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 US that impose requirements on data owners with respect to their service providers. There are, however, specific laws that address this issue, such as:

HIPAA
Through the Privacy and Security Rules, HIPAA imposes significant restrictions on the disclosure of PHI. The regulations require covered entities to enter into business associate agreements containing statutorily mandated language before PHI may be disclosed to a service provider.

GLB
In accordance with the Privacy Rule enacted pursuant to GLB, prior to disclosing consumer non-public personal information 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 pursuant to GLB, prior to 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.

State information security laws
A number of 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.

33 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

A wide variety of laws contain disclosure restrictions targeted to specific forms of PII. For example, HIPAA and GLB impose limitations on certain disclosures, such as requirements for consent and for contracts with certain types of recipients.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

US privacy laws do not impose restrictions on cross-border data transfers. The EU–US and Swiss–US Privacy Shield frameworks permit the transfer of personal data from the European Union and Switzerland to the United States. They also regulate the onward transfer of personal data from the United States to third countries through the use of onward transfer agreements, which are contracts that contain specific provisions regulating the use and disclosure of personal data by the onward transfer recipients of such data.

35 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

US privacy laws do not impose restrictions on cross-border data transfers.

36 Further transfer

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.

Rights of individuals

37 Access

Do individuals have the right to access their personal information held by PII 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 US 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, including:

HIPAA
Under the Privacy Rule enacted pursuant to HIPAA, an individual has a right to access 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:

(i) 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
(ii) allow such individuals the right to opt out of most third-party sharing.

If an organisation implements option (i), it must provide California residents with a postal address, email address or toll-free 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.

COPPA
This law allows parents or legal guardians to obtain access to the personal information that has been collected online from their children.

38 Other rights

Do individuals have other substantive rights?

The California Consumer Privacy Act provides consumers with the right to delete the personal information that the business has collected about 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. In addition, some sector-specific laws provide other substantive rights. For example, the HIPAA Privacy Rule does provide 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 FCRA provides individuals with the right to dispute and demand correction of information about them that is held by consumer reporting agencies.

39 Compensation

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 in order 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 FTC Act, for example, equitable relief is available first but then monetary penalties could reach $41,484 per violation for a breach of a consent order. Pursuant to 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 $100 and not more than $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.

HUNTON ANDREWS KURTH

Lisa J Sotto **lsotto@HuntonAK.com**
Aaron P Simpson **asimpson@HuntonAK.com**

200 Park Avenue
New York
New York 10166
United States

Tel: +1 212 309 1000
Fax: +1 212 309 1100
www.HuntonAK.com

40 Enforcement

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

41 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

There is no law of general application regarding privacy and information security in the US, and thus there are no derogations, exclusions or limitations of general application as there are in other jurisdictions. CISA provides companies with liability protection for cybersecurity monitoring and defence practices. For example, CISA preempts 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 CISA.

Supervision

42 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

The ability of an organisation to appeal orders of a supervisory authority is highly contextual. In the 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.

Specific data processing

43 Internet use

Describe 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 FTC has issued a substantial amount of guidance in the area of online behavioural advertising, and industry has responded with a series of self-regulatory frameworks. Although not focused directly on cookies, there have been a number of 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 third-party website or online services, if the operator engages in that collection.

44 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

See question 6.

45 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

NIST 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. In addition, HHS has issued guidance on HIPAA and cloud computing, clarifying that covered entities and business associates must enter into business associate agreements with cloud service providers that store or process electronic PHI before storing records containing ePHI in a cloud computing facility.

Getting the Deal Through

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
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
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
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
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
Loans & Secured Financing
Mediation
Merger Control
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
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-Private Partnerships
Public Procurement
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
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-78915-010-0