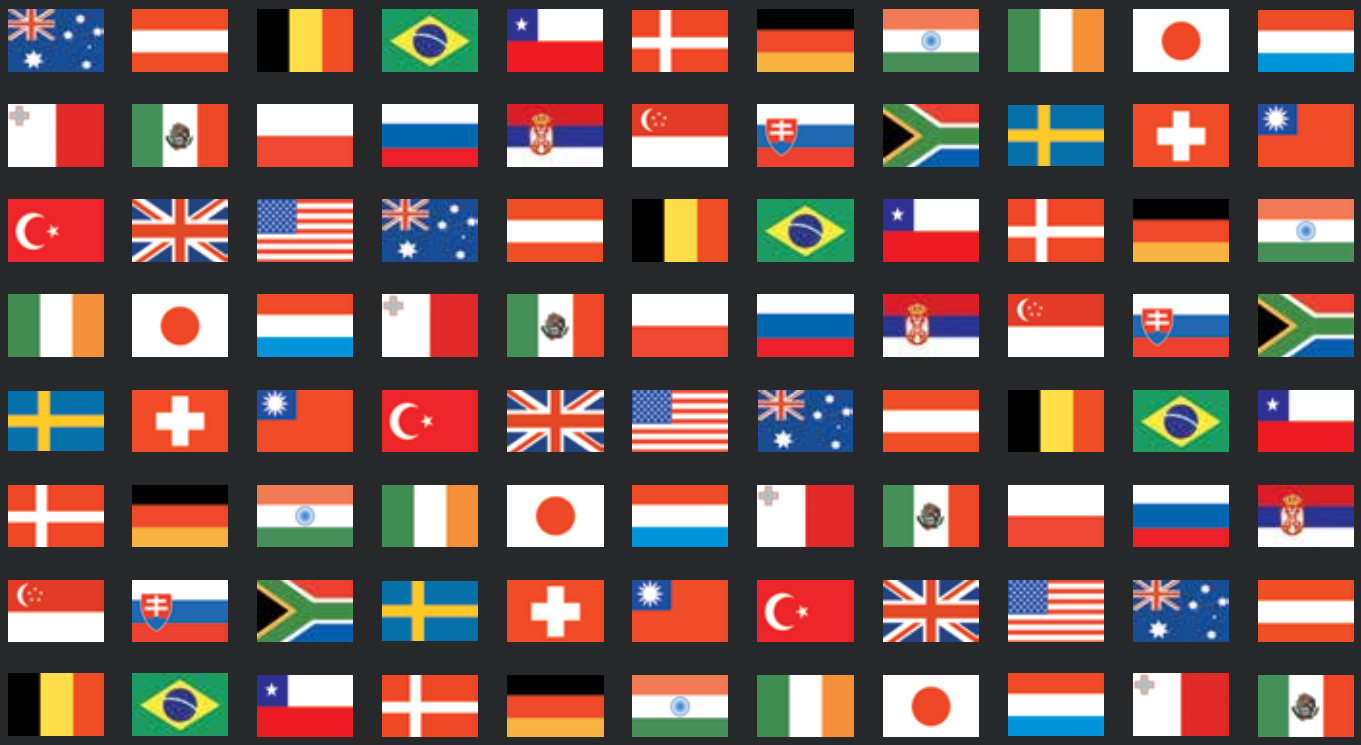
Data Protection & Privacy

Contributing editor
Wim Nauwelaerts



2017

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2017

Contributing editor
Wim Nauwelaerts
Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Fifth edition
ISSN 2051-1280

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

CONTENTS

Preface

Data Protection & Privacy 2017

Fifth edition

Getting the Deal Through is delighted to publish the fifth 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 Australia, Serbia and Turkey.

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 would like to thank and acknowledge Rosemary P Jay, of Hunton & Williams, whose tenure as contributing editor of the past four editions has shaped the publication to date. We also extend special thanks to the contributing editor, Wim Nauwelaerts, of Hunton & Williams, for his assistance with this volume.

GETTING THE DEAL THROUGH

London
August 2016

Introduction

Wim Nauwelaerts
Hunton & Williams

Introduction

Consistent with previous years, when my colleague Rosemary Jay was the editor of this publication, this introductory piece aims to highlight the main developments in the international privacy and data protection arena. 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 evermore 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 make sure to 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. This became clear in 2015 during the 37th International Conference of Data Protection and Privacy Commissioners in Amsterdam, where a report on 'building privacy bridges' between Europe and the US was presented, but which unfortunately recommends no substantive changes in law.

Privacy and data protection rules are inevitably influenced by legal traditions, cultural and social values, as well as 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 processing of personal information (eg, about consumers or employees). Although it makes absolute sense for global businesses to implement common standards for privacy and data protection throughout their organisation and regardless of where personal information is collected or further processed, there will always be differences in local 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 (the OECD Guidelines), the European Union Data Protection Directive 95/46/EC (the Directive), 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 49 countries: in June 2016 the Republic of Mauritius became the second non-European country, after Uruguay in 2013, to ratify Convention 108. Another three countries: Morocco, Senegal and Tunisia, have been invited to accede to Convention 108 and are expected to be the next countries to become parties. Cape Verde has taken the first steps to become a party as well. 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. The Convention's text is currently being updated to ensure that its data protection principles can stand the test of time.

The OECD Guidelines are not subject to a formal process of adoption but were adopted 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 European Union 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 the Directive, which was implemented by the EU member states with a view to creating an EU-wide framework for harmonising data protection rules. The Directive remained the EU's governing instrument for data protection until the General Data Protection Regulation was adopted in April 2016.

In 2004 these instruments were joined by a newer international instrument in the form of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. 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 for data transfers outside of the EU.

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 cyber security 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 eight African countries, and it has been reported that a number of African countries are planning to introduce 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. In the EU each member state has introduced legislation based on the Directive, which made it mandatory for member states to transpose the Directive's data protection principles into their domestic 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 ePrivacy Directive).

The data protection laws of the EU member states, the three associated states in the European Economic Area (ie, Iceland, Liechtenstein and Norway) and EFTA-country Switzerland broadly follow the same pattern, since they are all based on or at least inspired by the Directive. However, because the Directive is not directly applicable, the transposing member state laws tend to vary in some areas. This has led to inconsistencies, which create complexity, legal uncertainty and administrative costs for businesses that have to deal with 31 different data protection laws in Europe.

This is one of the reasons why the European Commission put forward its EU Data Protection Reform in January 2012, which included proposals for a General Data Protection Regulation (the Regulation) and a Data Protection Directive for the police and criminal justice sector (the Police and Criminal Justice Data Protection Directive). The idea behind the Regulation is that it will establish a single set of rules directly applicable throughout the EU, which would ultimately make it simpler and cheaper for companies to do business in the EU. It was estimated by the European Commission that one single law on data protection would do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year.

After four years of painful negotiations, on 15 December 2015, the European Parliament, the Council of the EU and the European Commission reached agreement on a new and arguably more harmonised data protection framework for the EU. The Council and the Parliament adopted the Regulation (EU 2016/679) and the Directive (EU 2016/680) in April 2016, and the official texts were published the following month. While the Regulation entered into force on 24 May 2016, it shall apply from 25 May 2018, allowing for a two-year transition period and repealing Directive 95/46/EC. The Police and Criminal Justice Data Protection Directive entered into force on 5 May 2016 and EU member states have to transpose it into their national law by 6 May 2018.

The adoption of the Regulation, which will be further discussed in this publication, is considered to be a 'game changer' and probably one of the most significant developments in the history of EU data protection law. The impact of the Regulation will not be confined to businesses based in the EU. The new rules will 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. This ambitious approach to jurisdiction, coupled with the potentially high level of fines (calculated on worldwide revenues) has ultimately prevailed, notwithstanding the plethora of concerns raised outside as well as within the EU.

In April 2016, the European Commission launched a public consultation on the controversial review of the ePrivacy Directive. This review, which intends to pursue consistency between the ePrivacy Directive and the Regulation, has raised questions about whether it is still necessary and meaningful to have separate rules on 'e-privacy', now that the Regulation has been adopted. To avoid legal uncertainty, it is essential that the review of the ePrivacy Directive is at least fully aligned with the Regulation and that any provisions that are overlapping with the Regulation are removed.

In addition to overhauling 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 applaudable 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 with the cybersecurity 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 like 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 is expected to enter into force in August 2016, but member states will have 21 months to transpose the Directive into their national laws. Thus far industry reactions to the NIS Directive have been lukewarm, mainly due to concerns that the NIS Directive is only scratching the surface of the issue.

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. It has also adopted specific privacy rules for health-related data: the Health Insurance Portability and Accountability Act (HIPAA). There are current proposals for further developments in US law, although whether all of them will ultimately become effective remains to be seen. 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 issued guidelines and procedures for sharing information under CISA. President Obama signed the Judicial Redress Act 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 April 2016, the US House of Representatives passed the Email Privacy Act in an attempt to modernise the way in which electronic communications can be used for purposes of criminal investigations. Finally, the White House released its Big Data report in May 2016, which identifies the benefits and risk of Big Data and includes recommendations on how to create Big Data standards for both the public and private sector.

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 scheme was heavily criticised in the EU following the Snowden revelations. On 6 October 2015, in what is considered a landmark decision, the Court of Justice of the European Union declared the Safe Harbor scheme invalid. This decision forced thousands of businesses that used to rely directly or indirectly on the Safe Harbor scheme to look for alternative ways for transferring personal information from the EU to the US. To address the legal vacuum that was created following the invalidation of 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. However, even before it was formally approved, the EU data protection authorities gathered in the Article 29 Working Party identified fundamental shortcomings with respect to the level of protection offered by the Privacy Shield. It remains to be seen whether the Privacy Shield will be able to live up to the expectations of the EU and US governments as well as the many businesses that will depend on it for their transatlantic data transfers.

In the Asia-Pacific region the early adopters of privacy and data protection laws – Australia, New Zealand and Hong Kong – have been joined in recent years by Malaysia, Singapore and South Korea. Australia has also strengthened its regime with the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and the APEC Privacy Framework is now supported by the APEC Cross Border Privacy Rules. China has reportedly been working on a cybersecurity bill, which would require data collected by 'critical infrastructure' operators to be kept within the country. 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 are expected to take effect in September 2017). The Personal Data Protection Standard in Malaysia came into force in December 2015 and complements the existing data protection law. In the Philippines, the implementing rules for the Data Privacy Act of 2012 were published in June 2016, and a national data protection authority was appointed around the same time. 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.

South America has seen the passage of laws in Argentina, Uruguay, Columbia, Chile and Peru with data protection laws in Argentina and Uruguay being modelled after the EU approach. Other South American countries, although they have not (yet) enacted EU-style data protection laws, have some degree of constitutional protection for privacy, including a right to habeas data, for example, Brazil and Paraguay. In May 2016, Brazil passed a decree that establishes rules for storing and protecting data held by internet service providers (the Marco Civil da Internet).

The global gaps in coverage lie in Africa and, to some extent, the Middle East. There are, however, some laws in both regions. As noted earlier, the African Union adopted a Convention on Cyber Security and Personal Data Protection in June 2014. The Convention has, however, been criticised as both vague and insufficiently focused on privacy rights. An increasing number of African countries are implementing data protection laws and cyber security regulations irrespective of the Convention. Angola, for example, passed its data protection law in 2011 and has recently approved a draft law creating a data protection authority. South Africa has passed law based on EU standards but it is not yet fully in force. In October 2015, the South African government created a virtual national cybersecurity hub to foster cooperation between the government and private companies. Tanzania passed its Cyber Crime Act in September 2015, and also the Ugandan government recently issued guidance and best practices in the cybersecurity field. Uganda plans to adopt its first privacy and data protection bill within the next year.

In the Middle East there are several laws that cover specific centres but, apart from Israel and Turkey, no country yet has comprehensive data protection law. Turkey adopted its first comprehensive data protection legislation (the Personal Data Protection Act) in March 2016.

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 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 serve as a compass to those doing business globally and help them navigate the murky waters of privacy and data protection.

HUNTON& WILLIAMS

Wim Nauwelaerts **wnauwelaerts@hunton.com**

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 3 643 58 00
Fax: +32 2 643 58 22
www.hunton.com

EU overview

Wim Nauwelaerts and Anna Pateraki
Hunton & Williams

On 16 April 2016, the EU General Data Protection Regulation (GDPR) was adopted after four years of intense negotiations. The GDPR is the most significant change in EU data protection law since the enactment of the EU Data Protection Directive (Directive) in 1995. The GDPR will become effective on 25 May 2018, allowing businesses to use a two-year transition period to make sure that their data protection practices are up to the standards of the GDPR. The GDPR will replace the existing Directive along with EU member state laws on data protection, and will be directly applicable in all EU member states without the need for local implementation rules. The GDPR therefore aims at harmonising all data protection legislation applicable in the EU member states.

Impact on businesses
The GDPR largely builds on the existing core principles of EU data protection law and expands them further or introduces new concepts addressing the challenges of today's data-driven economy and strengthening the protections of individuals. In addition, the GDPR reforms the current body of EU regulators (the Article 29 Working Party) into an EU Data Protection Board (the Board) with new powers and responsibilities.

The most significant concepts of the GDPR affecting businesses are outlined below.

Personal data
The GDPR maintains the existing definition of personal data as any information relating to an identified or identifiable individual, and extends it to include location data, IP addresses and online identifiers, in particular when combined with unique identifiers. In addition, the existing definition of sensitive data (ie, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life) has been extended to include genetic and biometric data, as well as sexual orientation.

Pseudonymous data
The GDPR suggests that pseudonymisation of data (eg, key-coding) is a risk mitigating measure and requires that additional information used to re-identify individuals (eg, a pseudonymisation key) should be kept separately from the relevant data sets and be protected by appropriate security measures. Pseudonymous data remain personal data as re-identification of individuals cannot be excluded. Pseudonymous data should not be confused with anonymous data, which does not allow re-identification and to which the GDPR does not apply.

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 non-EU businesses, the GDPR applies when they 'target' individuals in the EU by offering them products or services, or monitor the behaviour of individuals in the EU. Many online businesses that were previously not directly required to comply with EU data protection rules will now be fully affected by the GDPR.

Risk-based approach
The GDPR imposes obligations on businesses that require a risk-based approach. Under the GDPR, a two-step approach should be applied depending on whether the processing of personal data carries 'risk' or 'high risk' for the privacy rights of individuals. The GDPR provides examples of what constitutes risky processing, such as processing that may give rise to identity theft or fraud, unauthorised re-identification, and the processing of sensitive data and children's data. Where the processing is likely to result in high risk for individuals, the GDPR requires that Data Protection Impact Assessments are conducted and, in case of a data breach, that affected individuals are notified. This risk-based approach is expected to help businesses calibrate their compliance efforts.

Accountability
Under the GDPR, businesses will be held accountable with regard to their data processing operations and compliance obligations. Data controllers and data processors will have to keep internal records of their data processing activities, a system that will replace the current requirements to register with EU member state data protection authorities. This record-keeping requirement does not apply to small and medium-sized businesses with less than 250 employees, unless their data processing activities are risky or frequent or involve sensitive data. In addition, the accountability principle requires that businesses implement robust data security measures, apply privacy by design at an early stage of product development (eg, by implementing pseudonymisation and data minimisation techniques), and perform Data Protection Impact Assessments. Furthermore, in some cases a Data Protection Officer will need to be appointed, for example, if the 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 will 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. A mandatory data breach notification requirement does not currently exist in most EU member states, except for limited cases such as in Germany and the Netherlands. Under the GDPR, data controllers must notify data breaches to the regulators without undue delay and, where feasible, within 72 hours after becoming aware of the breach. 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 must notify affected individuals if the breach is likely to result in high risk to the individuals' rights and freedoms. The Board is mandated under the GDPR to issue guidance as to what constitutes high risk in this context. Businesses will face the challenge of developing data breach response plans and taking other breach readiness measures to avoid fines and negative publicity associated with data breaches.

Data processing agreements
The GDPR imposes minimum language that will need to be included in agreements with data processors. That minimum language is much more comprehensive compared to that 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, appropriate data security measures, audits and inspections, and an obligation to delete or return the data to the data controller upon termination of the services relating to the data processing. In addition, data processors must secure the prior authorisation of the controller, specific or general, before engaging sub-processors and enter into an agreement with sub-processors imposing on the sub-processor the same obligations that were imposed on them by the data controller. The

new requirements for data processing agreements will require many businesses to review and renegotiate existing vendor agreements.

Consent
The GDPR strengthens the conditions for obtaining individuals' consent as a legal basis for processing personal data. Consent must be based on 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 will not be valid for the purpose of the GDPR. Also, consent is unlikely to be valid where there is a clear imbalance between the individuals and the data controller seeking the consent. Electronic consent is acceptable, but it has to be clear, concise and not unnecessarily disruptive to the service. The GDPR explicitly confirms the currently applicable best practice that the provision of a service must not be made conditional on individuals providing consent to the processing of their data. In the context of online services directed to children, the GDPR requires parental consent for children below the age of 16, unless EU member state law prescribes a lower age limit. Given the stringent consent regime in the GDPR, businesses relying on consent for their core activities should carefully review their consent practices.

Privacy notices
Under the GDPR, privacy notices must be drafted in clear and plain language to enhance transparency for individuals. Privacy notices should also be provided in a concise, transparent, intelligible and easily accessible form. In addition to the information that privacy notices must include under the current regime, the GDPR requires that privacy notices specify the legal basis of the processing, the existence or absence of an adequate level of protection in third countries where the data are transferred, and the data transfer mechanism that businesses have implemented. The GDPR encourages the use of standardised, machine-readable icons to provide notice about the processing, as long as such icons provide a meaningful overview of the processing in an easily visible, intelligible and clearly legible manner. In the context of services directed to children, privacy notices should be drafted in clear and plain language that children can easily understand. The new transparency requirements of the GDPR will lead businesses to review their privacy notices and disclosures.

Data transfers
The GDPR maintains the general prohibition of data transfers to countries outside 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: going forward regulators will also be able to adopt Standard Contractual Clauses. Under the GDPR, it is no longer required to submit copies of executed Standard Contractual Clauses to data protection authorities for their review or approval (in the member states where this was previously required), which is a major improvement over the previous system. In addition, the GDPR formally recognises Binding Corporate Rules (BCRs) that will now be approved by regulators via the consistency mechanism. BCRs are privacy and data protection policies used by businesses to transfer personal data to group members outside of the EU, in compliance with EU data transfer restrictions.

Rights of individuals
The GDPR largely maintains the existing rights of individuals, and introduces additional rights. For instance, the GDPR strengthens the right of individuals to object to possible negative effects of automated decision making based on profiling, which is expected to impact the consent practices of a variety of online and mobile businesses. 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 the processing does not or no longer complies with the GDPR or relates to children's data in the online context. Furthermore, the GDPR introduces the right to data portability, based on which individuals can request to have personal data returned to them or transmitted to another service provider 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 will need to review their existing practices with regard to addressing individuals' requests and consider how they will give effect to the new rights.

One-stop shop
One of the most significant new concepts of the GDPR is the one-stop shop. The GDPR allows businesses to have multi-jurisdictional data protection issues monitored and enforced by one supervisory authority (SA) acting as a lead SA. Businesses can therefore have a one-stop shop regulator who will be acting as their single contact point. In addition, the GDPR introduces a detailed cooperation and consistency mechanism, in the context of which SAs should exchange information, conduct joint investigations, and coordinate actions in relation to draft enforcement decisions proposed by the lead SA. In case of a dispute among SAs with regard to draft enforcement decisions, the matter can be escalated to the Board for a binding decision. Purely local complaints without a cross-border element can be handled by the relevant local SA, after the lead SA has been informed and has agreed to that course of action. Although the initially proposed one-stop shop concept has been weakened following intense debate during the legislative process, it remains one of the most important innovations introduced by the GDPR .

Administrative fines
The GDPR introduces high administrative fines that will significantly change the currently fragmented enforcement landscape. EU member state regulators will be able to 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, cooperation of supervisory authorities will increase under the GDPR, which is expected to lead to more coordinated enforcement action.

The GDPR will set the stage for a more robust and mature data protection landscape in the EU for the foreseeable future. It will apply to virtually any business dealing with personal data relating to individuals in the EU. Businesses should take advantage of the two-year transition period (until May 2018) to adapt to the new challenges and increase the level of maturity of their privacy compliance programmes.

HUNTON& WILLIAMS

Wim Nauwelaerts **wnauwelaerts@hunton.com**
Anna Pateraki **apateraki@hunton.com**

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

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

Safe Harbor and the Privacy Shield

Aaron P Simpson
Hunton & Williams

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, especially in the wake of Edward Snowden's explosive revelations in 2013 regarding government snooping. 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. The invalidation of Safe Harbor has 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 as of July 2016 has been formally approved in Europe.

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-twentieth century Europe, the region takes an understandably hard line approach to data protection. The processing of personal data about EU citizens is, at the time of publication, strictly regulated through Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive is implemented by the member states of the EU, which impose onerous obligations through their national laws regarding the collection, use, sharing and safeguarding of personal data, both locally and extraterritorially. This legal landscape is in the midst of change, as the General Data Protection Regulation will be replacing the Directive in May 2018. While the General Data Protection Regulation will usher in a host of new changes, the hard line approach to data protection will continue.

These 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 Safe Harbor 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 import 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 invalided in October 2015.

Invalidation of the Safe Harbor framework

Criticism of the Safe Harbor framework from Europe began in earnest in 2010. In a large part, the criticism stems from the perception that the Safe Harbor is 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. 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, 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 Article 29 Working Party, which is the group of European Union Member State Data Protection Authorities, subsequently offered its support, albeit tepid, for the new framework.

HUNTON& WILLIAMS

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

200 Park Avenue
New York
New York 10166
United States

Tel: +1 212 309 1000
Fax: +1 212 309 1100
www.hunton.com

Australia

Alex Hutchens, Jeremy Perier and Eliza Humble
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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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). 'Personal information' is the conceptual equivalent of 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 general 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 collection, use, storage, disclosure and destruction of personal information.

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 6), and other legislation at the commonwealth and state level that are relevant to privacy and the use of personal information, including the Spam Act 2003 (Cth) (Spam Act), which regulates electronic marketing, 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 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$1.8 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 may:

- issue a formal warning;
- require an entity to give a court-enforceable undertaking, the breach of which can lead to 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$1.8 million for repeated breaches of the Spam Act.

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 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$1.8 million 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.

While there is no mandatory requirement to notify the Information Commissioner of any breach, if there is a real risk of serious harm as a result of a data breach, it is best practice to notify both the affected individuals and the Information Commissioner. It is an important mitigation strategy for APP entities and can promote transparency and trust in the APP entity.

Scope

4 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. 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 (annual turnover 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.

5 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).

6 Other laws

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

In Australia, 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
- Healthcare Identifiers Act 2010 (Cth), which regulates the use and disclosure of healthcare identifiers.

The telecommunications sector is also subject to specific data protection rules, including in 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.

7 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.

8 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.

9 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?

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 normally expect to have.

Legitimate processing of PII

10 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.

11 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 is 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

12 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. APP5 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 or tribunal order;
- the purposes for which the information is collected;
- any other person to whom 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.

13 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 12). 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 form the individual on a recurring basis.

14 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 10, 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).

15 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, with 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, size, resources, 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.

16 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 or tribunal order to retain the personal information).

17 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 privacy policy of the APP entity.

18 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 in question 17, 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 (eg, tax file numbers or social security numbers).

Security

19 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 controls 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.

20 Notification of data breach

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

As of July 2016, there is no mandatory notification obligation regarding data breaches in the Privacy Act. However, a draft bill relating to data breach notifications has been issued and was originally intended to be passed into law in late 2015. It is expected that this will be reintroduced following the general election in July 2016 and so the situation may change over the ensuing months.

In the meantime, the Information Commissioner has released a guide to handling personal information security in which it is highly recommended 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

21 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 at least have a person or department responsible for matters related to data security and privacy. This person or department would be the first point of contact for any queries or complaints from the public or the Information Commissioner.

22 Record keeping

Are owners 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, APP5 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.

Registration and notification

23 Registration

Are PII owners and/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.

Update and trends

Australian data protection law is an area of key regulatory focus. In August 2016, a key decision of the Federal Court is expected, which will determine whether or not an IP address is personal information. Also, following the introduction of mandatory metadata retention laws for telecommunications carriers, it is expected that mandatory data breach notification laws will be introduced (this was part of the political negotiation to pass the data retention laws). The general election in July 2016 delayed the introduction of the laws, but it is expected that whichever party wins the election, the laws will be introduced.

Also, there are other key regulatory reforms that are perennially debated. The most likely to be introduced in the medium term are the removal of the employee-records exemption, the removal of the small-business exemption, and the introduction of an actionable statutory right to privacy (similar to that which exists in Europe).

24 Formalities

What are the formalities for registration?

No registration fee is payable.

25 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.

26 Refusal of registration

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

Not applicable.

27 Public access

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

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

28 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.

Transfer and disclosure of PII

29 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 data 'controller' and 'processor', therefore 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 31.

30 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).

31 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 overseas-based persons 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.

32 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.

33 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

34 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 request can be refused, including where it would pose a serious threat to the life, health and 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.

35 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 that 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.

36 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 or seek civil penalty orders before the Federal Court of up to A$360,000 for individuals and up to A$1.8 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.

37 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, which may then take appropriate actions such as investigating the complaint or seeking a court order.

Lawyers | McCullough Robertson

Alex Hutchens **ahutchens@mccullough.com.au**
Jeremy Perier **jperier@mccullough.com.au**
Eliza Humble **ehumble@mccullough.com.au**

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

Tel: +61 2 8241 5600
Fax: +61 2 8241 5699
www.mccullough.com.au

Exemptions, derogations and restrictions

38 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

39 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

40 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. At a minimum, this means describing cookie-based marketing activity in a privacy policy.

Also, it is 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 and signatories include leading domestic and international digital businesses.

41 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 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.

42 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 onto 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.

Austria

Rainer Knyrim

Preslmayr Rechtsanwälte OG

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The legislative framework for the protection of personally identifiable information (PII) in Austria mainly consists of the Data Protection Act (ADPA). In addition, 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 Labour Constitutional Act regarding data applications for purposes of personnel administration and evaluation. In the field of health care 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 ADPA was enacted in 2000, implemented the EU Data Protection Directive 95/46/EC (the Directive) and regulates which types of personal data may be processed by whom and under which circumstances and conditions. In addition, it should be noted that the right for the protection of personal data has constitutional status in Austria.

2 Data protection authority

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

The competent, and monocratic, authority is the Data Protection Authority (DPA). The DPA is an independent authority and ensures that individual rights and interests in secrecy of personal data are protected.

The DPA decides on notifications of data applications, applications for authorisations of data transfers to countries outside the European Economic Area (EEA) as far as those countries do not provide an adequate level of protection and functions as a complaint authority for anyone whose rights for privacy or data protection have (allegedly) been infringed.

In case of an alleged infringement the DPA is able to request detailed information from controllers or processors, has the power to carry out audits of data applications, on-site inspections and may issue recommendations. Furthermore, the DPA is empowered to report an offence to the department of public prosecution or to file claims with the responsible court in case of severe infringements of data protection law.

3 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 regulations can lead to criminal or administrative penalties. Any individuals that – with the intention of profiting or harming others – use, make available to others or publish personal data entrusted to or accessible to them solely due to professional reasons or that they acquired illegally, will be punished by court with imprisonment of up to one year, unless the offence is subject to 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).

Anyone who commits any of the following may be punished with a fine of up to €25,000:

- intentionally and illegally gains access to a data application or keeps up an obvious illegal access;
- intentionally transmits personal data in violation of the rules on confidentiality and, in particular, misuses data entrusted to him or her pursuant to the provisions granting the use of personal data for scientific research and statistics or of address data to inform or interview data subjects for other purposes;
- uses personal data or fails to grant access to such data to rectify or to erase it in violation of a valid judicial or administrative decision;
- intentionally erases personal data in violation of section 26, paragraph 7 ADPA; or
- intentionally acquires personal data in case of disaster under false pretences violating section 48a ADPA.

Anyone who commits any of the below offences may be punished with a fine of up to €10,000:

- collects, processes or transfers personal data without fulfilling his or her notification duty for data applications or video surveillance or operates a data application that deviates from his or her filing;
- transfers personal data abroad without a required prior approval of the DPA;
- infringes commitments given to the DPA or infringes stipulated constraints;
- infringes his or her disclosure and information duties to data subjects;
- grossly infringes his or her duty to implement appropriate data security measurements pursuant to section 14 ADPA;
- infringes his or her duty not to perform automatic image matching on video surveillance material, not to scan surveillance material for sensitive data automatically or to log the utilisation of surveillance material; or
- infringes his or her duty to delete surveillance material after its legal retention period.

In addition, anyone who fails to grant access to personal data, to rectify or to erase personal data in violation of the ADPA, unless the offence is subject to more severe punishment pursuant to another provision, may be punished by a fine of up to €500.

Scope

4 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 personal data, 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.

5 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 personal data, the provisions of the 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 Labour Constitutional Act, which, to the extent of the respective provisions, also forms part of Austrian data protection law. Video surveillance as well as analysing protocol data to assess the behaviour of data subjects is also covered by the ADPA.

6 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 ADPA. 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 personal data. 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 personal data across multiple authorities. If smart meters are used for the supply of electricity or gas the applicable acts contain provisions for the protection of personal data 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).

7 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. Moreover, the ADPA not only protects the personal data of natural persons but also that of legal persons and groups of persons (eg, unincorporated bodies).

8 Extraterritoriality

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

The ADPA applies to the use of personal data in Austria, and outside Austria insofar as the data are 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 personal data 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 are only transmitted through Austrian territory.

9 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?

Austrian data protection law gives broad cover to the processing of personal data; any type of processing such as collecting, storing, transferring, viewing, giving access, etc, is covered by its provisions. A very important distinction is made, in practice, between the transfer of personal data and the mere 'handover' of data to a third party for the sole purpose of the provision of services to the controller. If the receiver of the data uses the data for its own purposes, then data is regarded as having been transferred. In most cases, a transfer of personal data must be notified with the DPA and there are certain underlying restrictions (eg, the transfer has to serve a legitimate purpose of the recipient; and a transfer to outside the EEA has to be authorised by the DPA, unless certain exemptions as mentioned in question 31 apply).

In general, a commitment of data to a service provider does not have to be notified with the DPA, but the commitment of a service provider established outside Austria must be governed by a written contract between the data controller and the data processor that especially regulates the handling of data by the service provider. Moreover, if the service provider is established outside the EEA, the DPA's authorisation for the committing of the data is necessary, unless one of the exemptions applies, as mentioned in question 31.

Legitimate processing of PII

10 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?

Austrian data protection law requires a legitimate purpose and a legal basis for each processing and transmission of personal data. Four major possible legal bases are provided by the ADPA:

- processing is required to comply with the law;
- data subjects have given their explicit consent;
- processing of data is required for the vital interests of the data subject (or others); and
- the interests of the controller in the processing of data prevail over the legitimate interests of the data subject in the concealment of his or her data (eg, for contract fulfilment or the exercise of rights before authorities or courts).

11 Legitimate processing – types of PII

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

There are four specific types of data for which more stringent rules are applicable:

- sensitive data (ethnic origin, political opinions, membership in unions, religious or philosophical views, health and sex life);
- data related to criminal convictions;
- data that is processed to provide information on the creditworthiness of the data subject; and
- data being part of a joint information system (jointly processing of data in one data application by several controllers).

Data handling responsibilities of owners of PII

12 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 ADPA obliges data controllers collecting data to inform data subjects about the purposes of the data application as well as about the data controller's name and address, if this information is not available to the data subject. If data controllers process data within a data application that is subject to registration (see question 23), their registration number must be provided to data subjects. Further information has to be provided appropriately, as far as is necessary for data to be processed in good faith, especially if the data subject has the right to object the processing of its data (eg, to the transmission of marketing material), if it is ambiguous for the data subject whether he or she is legally obliged to provide the requested data or if data are processed within a joint information system.

If the data controller operates a video surveillance system, monitored areas have to be marked with appropriate signs in order to enable individuals to avoid entering observed areas.

13 Exemption from notification

When is notice not required?

There is no notice required if data is processed in a data application that is exempted from notification. A data application is exempted from

notification if it is completely operated according to a 'standard application'. Standard applications are regularly published as a regulation by the Federal Chancellor of Austria and list personal data that may be legitimately processed for designed purposes; in addition, the exemption only applies if the data are transferred to those categories of recipients named in the relevant standard application.

Furthermore, an application is exempted from notification if:

- only legitimately published personal data are processed;
- the application implements a publicly accessible register or directory established pursuant to a legal provision;
- only pseudonymous personal data are processed (the controller is not able to identify data subjects);
- the application is operated for private or family purposes only; or
- the application is operated for journalistic purposes.

Exemptions also exist for data applications serving one of the following purposes:

- protection of the constitutional establishments of the Republic of Austria;
- safeguarding the operational readiness of the Austrian Army;
- safeguarding the interests of a comprehensive national defence;
- protection of important foreign policy, economic or financial interests of the Republic of Austria or the European Union; or
- prevention and prosecution of crimes, as far as is necessary to meet these purposes.

14 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 controller of personal data must provide data subjects with access to their data. Upon the data subject's request, the controller has to rectify or even erase the data, unless the controller has a legitimate interest regarding the processing of the data. If a deletion or correction of personal data cannot be carried out immediately but for reasons of economy only at specific times (eg, the next backup routine), access to data to be deleted must be blocked and a correction note must be added to the data that is to be corrected.

15 Data accuracy

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

As soon as data are collected and stored, the data controller has the obligation to ensure that the data are always correct and kept up to date, as long as their accuracy is necessary to fulfil the intended purposes. In addition, the controller has to ensure that data are only stored as long as necessary for the legitimate purpose of their processing, and as long as both the purpose and the legal basis for the processing exist with respect to any particular individual that is subject to the application (eg, the individual might withdraw his or her consent, the employee might have left the company).

16 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 restricts the amount of data held by establishing the principles of data minimisation, which means that only those data may be held that are absolutely necessary and essential for the achievement of the purpose for which the data are collected. Similarly, data may only be held for the amount of time necessary for the purpose and as long as required by law (if applicable). Otherwise, data has to be deleted physically as a logical deletion is not sufficient (eg, if the respective data are only marked as being deleted in the database or if only the respective indices in the file system are removed).

17 Finality principle

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

A purpose limitation principle (in the sense that the processing of data is only legitimate for specific purposes) has been adopted. The processing of data is allowed for any legitimate and valid purpose.

18 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 purpose has to be evaluated individually for every single case. Often, a balancing of the controller's interests with those of the data subject is necessary and delivers the answer whether the use of personal data is legitimate or not. If personal data shall be used for other application purposes of a controller (eg, another business domain) any further use has to be treated like a data transmission to other data controllers. Therefore, any such further use must fulfil the legal requirements equal to a data transmission but there is an exemption for scientific or statistical purposes, for which personal data may be used under certain conditions.

Personal data may be further used for scientific and statistical purposes under one of the following conditions:

- the data is publicly available;
- the data was initially collected legitimately by the controller for other purposes;
- the data are used only in a pseudonymous form;
- the data are used for these purposes pursuant to a legal provision;
- the data subject has given his or her consent; or
- the DPA has given its approval.

Nevertheless, also in case of a legitimate use of personal data for scientific or statistical purposes according to one of the conditions mentioned above, this data has to be transformed into a pseudonymous form immediately if pseudonymous data is sufficient to serve the research's purposes as well. As long as it is not stated otherwise by law, data must be anonymised immediately if the personal identity of the data subjects concerned is no longer relevant.

Security

19 Security obligations

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

Controllers and processors must apply state-of-the-art security measures to protect data against accidental or intentional destruction or loss. Furthermore they must ensure that data are properly used and are not accessible to unauthorised persons.

The imposed security obligations in particular are as follows:

- distribution of functions between the organisational units, as well as the operatives regarding the use of data, has been laid down expressly;
- use of data has been tied to valid orders of the authorised organisational units or operatives;
- every operative employee has been instructed about his or her duties of confidentiality pursuant to the ADPA and to internal data protection regulations including data security regulations;
- operation of an access control system for objects of the data controller or data processor;
- operation of an access control system for the protection of data and programs as well as for the protection of storage media against unauthorised access and use;
- the permissions to operate data processing equipment have been defined and every device has been secured against unauthorised operation by taking security measurements for the machines and programs used;
- creation of log files in order to monitor the legitimacy of the use of personal data like retrieval, modifications and transmissions; and
- establishment of an appropriate documentation about the measures taken pursuant to the previous bullet points to facilitate control and conservation of evidence.

Although all these security measures to be taken seem very comprehensive, they usually do not impose a large burden on data controllers as they are only obliged to take security measures as long as they are economically justifiable. Furthermore security measures are generally only scrutinised by the DPA in case of complaints.

20 Notification of data breach

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

The ADPA stipulates a 'data breach notification' duty for controllers that have failed to keep their processed data secure; if the controller becomes aware of any systematic and grave misuse of any data that might cause harm to the affected data subjects, the controller has the obligation to adequately inform the data subjects thereof. This obligation is usually fulfilled by written statements to the subjects, which provide them with the information of the security breach, the data affected, any recipient of the data (if known) and the possible dangers resulting from the breach. If only minor damage is supposed and the information of the subjects would cause inappropriate costs or effort then controllers must not inform the data subjects. There is no provision within the ADPA to inform the DPA of any breach.

On the contrary the Telecommunications Act obligates providers of public communication services to notify any case of a personal data breach to the DPA without delay. Within the notice to the DPA providers of public communication services must already describe the consequences of the data breach and measures proposed or taken to address the data breach. In cases where it is likely that the privacy of individuals is adversely affected, individuals must be noticed too. The notice to the persons affected must describe the nature of the personal data breach, contact points to obtain more information and recommendations to mitigate the effect of the data breach.

Internal controls

21 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. There are no rules for data protection officers within the ADPA.

22 Record keeping

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

Owners of PII are required to establish internal processes and documentation in order to ensure the rights of individuals regarding their data (see question 34). Equal measures have to be taken by all organisational units of a data controller or data processor that use data in order to ensure data security.

Registration and notification

23 Registration

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

Once a private company or a public authority processes personal data (relating to its employees, customers or any other natural or legal persons) it must register as a data controller and notify its data applications with the DPA. There are only a few exceptions from the registration duty, the most important of which are the 'standard applications', which are regularly published as a regulation by the Federal Chancellor of Austria and determine in detail which categories of data may be processed and transmitted lawfully. If a data application can be completely subsumed under such a standard application, the duty to notify or register is lapsed.

Further exemptions from the duty to notify a data application with the DPA are described in detail in question 13.

24 Formalities

What are the formalities for registration?

The data controller has to file a notification with the Data Processing Register by using an online application (DVR-Online), including information about the data controller's name, commercial register number, postal address, email address and telephone number. In addition, for each data application the data controller has to notify the purpose of the application, its legal basis, the categories of data subjects concerned, the data categories processed, all data security measurements implemented and, if any, recipients of personal data along with the data categories transferred to them. All this data has to be kept up to date and any changes have to be filed with the Data Processing Register immediately. If special categories of data are to be processed (see question 11), the DPA's authorisation is necessary before the data may be processed. No notification fees are charged.

25 Penalties

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

If an application is operated without being registered appropriately or without being registered at all, a fine of up to €10,000 may be imposed on the data controller.

26 Refusal of registration

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

The Data Processing Register may initiate an improvement process if the data controller's notification is found to be insufficient, incorrect or even unlawful. If the data controller does not improve its notification within the determined period, registration of the notification will be refused. In that case the data application must not be carried out.

27 Public access

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

The Public Data Processing Register may be consulted by anyone online at https://dvr.dsb.gv.at/.

28 Effect of registration

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

Once a data controller has registered with the Data Processing Register, it is obliged to keep any data updated and to inform the Data Processing Register of any new information or amendments to data notifications (see also question 12 et seq). If special categories of data are to be processed (see question 11), the DPA's prior authorisation is necessary. In addition the controller has to disclose its registration number (given by the DPA) in communications to data subjects (see also question 12).

Transfer and disclosure of PII

29 Transfer of PII

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

Controllers may employ processors for their data applications insofar as the latter sufficiently warrant the legitimate and secure use of data. Therefore, the controller must enter into the necessary agreements with the processor in order to ensure the data processor has all data security measurements implemented as required by law. Controllers must satisfy themselves that the agreements are complied with by acquiring the necessary information about the actual measures implemented by the processor.

Irrespective of further contractual obligations, all processors have the following obligations when processing personal data on behalf of the controller:

- data may only be used according to the instructions of the controller;
- compulsory data safety measures have to be taken (see question 19);
- sub-processors may only be engaged with the prior permission of the controller and the controller has to be informed of any intended engagement of a sub-processor;
- technical and organisational measurements have to be implemented for the fulfilment of the controller's obligation to grant the right of access, rectification and erasure;
- all results from the processing and all documentation data have to be returned to the data controller after the termination of service; and
- all information necessary for the data controller to enable him or her to examine if the data processor has discharged its obligations arising from the engagement has to be provided to the data controller.

30 Restrictions on disclosure

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

According to the ADPA, data must only be transferred if:

- they originate from a lawful data application;
- the recipient has demonstrated his or her statutory competence or legitimate interest with regard to the purpose of the transfer to the transmitting party; and
- the confidentiality of the data subject is not infringed by the purpose and content of the transmission.

To meet these requirements, data must only be used fairly and lawfully, only be collected for specific, explicit and legitimate purposes and be used insofar as they are essential for the purpose of the data application. In addition, data must only be processed insofar as the purpose and content of the data application are covered by the statutory competencies or the legitimate authority of the respective controller and the data subject's confidentiality is not infringed by the processing.

Non-sensitive personal data may be processed if one of the following conditions is met:

- an explicit legal authorisation or obligation exists to use the data;
- the data subject has given his or her consent, which can be revoked at any time, whereby such a revocation makes any further use of the data illegal;
- vital interests of the data subject; or
- prevailing interests pursued by the controller or by a third party require the use of data.

The use of legitimately published data and merely indirect (pseudonymous) personal data will not constitute an infringement of interests in confidentiality (the right to object to the use of such data remains unaffected).

If sensitive data is processed, confidentiality is not infringed if:

- the data subject itself has obviously made the data public;
- the data is used only in an indirect (pseudonymous) personal form;
- the obligation or authorisation to use the data is stipulated by law, insofar as it serves an important public interest;
- the data are used by a controller in the public sector in fulfilment of its obligation to give the authorities assistance;
- data is used that solely concerns the execution of a public office by the data subject;
- the data subject has given his or her unambiguous consent, which can be revoked at any time, whereby such a revocation makes any further use of the data illegal;
- the processing or transmission is in the vital interest of the data subject and his or her consent cannot be obtained in time;
- the use is in the vital interest of a third party;
- the use is necessary for the establishment, exercise or defence of legal claims of the controller before a public authority and the data were collected legitimately;
- the data is used for private, research or statistical purposes or in case of disaster;
- the use is required according to the rights and duties of the controller in the field of employment law and civil service regulations and is legitimate pursuant to specific legal provisions (the rights of the labour councils according to the Labour Constitution Act with regard to the use of data remain unaffected);
- the data is required for the purpose of preventive health care, medical diagnosis, the provision of health care or health treatment or the management of healthcare services, and the use of data is performed by a medical person or other persons subject to an equivalent duty of secrecy; or
- non-profit organisations with a political, philosophical, religious or trade union aim process data revealing the political opinion or philosophical beliefs of natural persons in the course of their legitimate activities, as long as these data concern members, sponsors or other persons who disclose an interest in the aim of the organisation on a regular basis; these data shall not be disclosed to a third party without the consent of the data subject unless otherwise provided for by law.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Data transfers from Austria to any other EEA member states are not subject to any additional requirements, as EEA member states are considered to provide an 'adequate level of data protection'.

Also, data transfers to recipients in third countries providing an adequate level of data protection do not need to fulfil any further requirements. All jurisdictions that are not a member of the EEA but provide an adequate level of data protection are enumerated in a regulation of the Federal Chancellor (Federal Law Gazette II No. 521/1999 as amended by No. 449/2015) and are listed here: Andorra, Argentina, Faroe Islands, Guernsey, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

Pursuant to this regulation, a data transfer to one of the following countries does not require the Data Protection Authority's prior approval, unless under specific conditions as stated in the regulation: Canada (in accordance with the Commission Decision 2002/2/EC) and Israel (in accordance with the Commission Decision 2011/61/EU).

Furthermore, any applicable decision of the European Commission is binding in Austria.

In any case, a transborder data exchange does not require the DPA's prior authorisation if:

- the data to be transferred has been published legitimately in Austria;
- only indirect personal (pseudonymous) data is transferred;
- the transborder transfer is authorised by legal provisions that are equivalent to a provision of the Austrian legal system and are immediately applicable;
- data originating from a data application for private or journalistic purposes are transmitted;
- the data subject has without a doubt given his or her consent to the transborder data transmission;
- a contract has been concluded between the controller and the data subject or the controller and a third party that is clearly in the interests of the data subject and that cannot be fulfilled without the transborder transmission of data;
- the transmission is necessary for the establishment, exercise or defence of legal claims before a foreign authority and the data was collected legitimately;
- the transmission is expressly mentioned in a standard application or model application;
- the data exchange is carried out with Austrian governmental ministries and offices in foreign countries; or
- the transmission concerns personal data out of a data application that is exempted from the notification duty pursuant to section 17, paragraph 3 ADPA.

If the transborder data exchange is not exempted from a prior authorisation duty, the controller has to apply for authorisation to the DPA. In the context of transborder data flows to countries that do not provide an adequate level of data safety, data transfer agreements are very important. To receive the DPA's approval for the transfer of personal data to these countries, it is necessary that the controller provides sufficient guarantees to ensure an adequate level of data protection. Such an adequate level of data protection could be established by the conclusion of data transfer agreements based on the European Commission's standard contractual clauses. A precise distinction needs to be made between controller-to-controller and controller-to-processor clauses. If such agreements are concluded using the standard contractual clauses as published by the European Commission, the probability of receiving the DPA's authorisation is quite high.

32 Notification of cross-border transfer

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

If a data application is not exempted from the duty of notification at all, data transfers have to be filed with the DPA as well. Such a notification has to be carried out together with the filing of the data application itself via the Data Processing Register. For those cases where a prior authorisation of the DPA is needed for international data transfers, see question 31.

33 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 to transfer data outside the jurisdiction also apply to data transfers to service providers or onwards transfers if the recipient is located outside the jurisdiction.

Rights of individuals

34 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 data processed by controllers and to receive a copy. The data controller is obliged to provide the data subject with information about personal data being processed, if the data subject has requested access in writing and proved his or her identity, as appropriate (eg, by transmitting a copy of his or her passport). If there is no reason to refuse a data subject's request, the desired information must be disclosed within eight weeks. If data controllers do not process data of the data subject that has requested information they must provide a 'negative information' to the data subject within eight weeks upon receipt of the request for information.

The first information per year per data subject has to be given free of any charge; for any exceeding requests for information, rate compensation may be charged.

Information shall not be disclosed to the data subject if this is necessary for the protection of the data subject because of special reasons or if legitimate interests pursued by the data controller or by a third party – especially overriding public interests – prevail providing the information. Prevailing public interests are the following:

- protection of the constitutional institutions of Austria;
- safeguarding the operational readiness of the Federal Army;
- safeguarding the interests of a comprehensive national defence;
- protection of important foreign policy, economic or financial interests of the Republic of Austria or the European Union; or
- the prevention and prosecution of crimes.

The review of the legitimacy of a refusal to provide the requested information for one of these reasons is subject to the DPA's decision.

35 Other rights

Do individuals have other substantive rights?

Besides the right of access, individuals have the right to apply for correction and deletion of personal data relating to them if this data is inaccurate. Finally, individuals have the right to raise objections to the data controller of a data application against the use of personal data because of infringement of the data subject's confidentiality arising out of any special situation.

36 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 demand compensation if they are affected by breaches of data protection law. A person who has been damaged by an infringement of provisions of the ADPA (confidentiality, correction, erasing) may bring a civil action for damages. In general, compensation may only be demanded for actual damages, but there is an exception, which states that a claim for appropriate compensation for the defamation suffered may be brought against a data controller if the personal data was used publicly in a manner that violated a data subject's interests in secrecy exposing that person to the extent similar to that described in the Media Act – even if public use of that data is not committed by publication in the media.

In case indications arise that a serious data protection infringement has been committed by a private sector controller, besides the data subject, the DPA is also empowered to file an action for a declaratory judgment with the responsible court.

Update and trends

Since the Privacy Shield as successor to the Safe Harbor Decision has not yet been enacted, international data transfer is still a hot topic among Austrian data controllers as more and more cloud services are used. Hence standard contractual clauses have become the instrument of choice in order to legitimately transfer data to countries outside the EEA.

Another hot topic is the upcoming application of the the General Data Protection Regulation. Due to the sanctions stipulated within the GDPR, data protection law has gained more significance among data controllers. Even thought the GDPR will only be applicable as of 25 May 2018, data controllers are already starting to look seriously for guidance on how to implement its provisions.

In order to provide as much guidance as possible, 34 privacy experts joined together and published the first practical guidance (Knyrim (Ed), *Datenschutz-Grundverordnung*) to help data controllers to understand and comply with the GDPR.

37 Enforcement

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

The rights of individuals are enforceable through either the DPA or the judicial system, but the responsibility depends on the right to be exercised and if the data controller is established by public or private law. Complaints against data controllers of the public sector have to be filed exclusively with the DPA as long as the complaint shall not be brought against organs of the legislative or jurisdiction. Claims against data controllers of the private sector must generally be filed with the responsible civil court except for complaints regarding an alleged infringement of the right to information, which must be filed with the DPA.

Anyone has the right to lodge an application with the DPA because of an alleged infringement of his or her rights pursuant to the ADPA by a controller or a processor (public or private sector). In case of an application the DPA can only issue recommendations to establish the rightful state.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

No.

Supervision

39 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

40 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 ADPA and the Telecommunications Act respectively. As the EU e-Privacy 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 e-Privacy Directive in November 2011 and has simply translated article 5, paragraph 3 of the Directive into section 96, paragraph 3 of the Telecommunications Act.

41 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.

42 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 ADPA are applicable. As cloud service providers are often located outside the EEA, international data transfer needs special attention (see question 31). Since the Safe Harbour Decision has been declared invalid by the ECJ, using cloud computing services outside the EEA now usually requires the conclusion of standard contractual clauses and their authorisation by the DPA as the proposed Privacy Shield is not yet enacted.

PRESLMAYR
RECHTSANWÄLTE

Rainer Knyrim **knyrim@preslmayr.at**

Universitätsring 12
1010 Vienna
Austria

Tel: +43 1 533 16 95
Fax: +43 1 535 56 86
www.preslmayr.at

Belgium

Wim Nauwelaerts and David Dumont
Hunton & Williams

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The main data protection legislation is the Act on the Protection of Privacy in relation to the Processing of Personal Data of 8 December 1992 (the Data Protection Act), as well as the Royal Decree of 13 February 2001 implementing the Data Protection Act (the Royal Decree). The Data Protection Act, which has been significantly amended over time, transposes Data Protection Directive 95/46/EC into Belgian law.

Furthermore, the following international instruments on privacy and data protection also apply in Belgium:

- 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).

In addition to the general legislative framework for data protection outlined above, there is also sector-specific legislation relevant to the protection of PII. The Electronic Communications Act of 13 June 2005 (the Electronic Communication Act), for instance, imposes obligations on telecom operators and internet service providers regarding the use of location data and the notification of data security incidents.

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, better known as the Privacy Commission, is responsible for overseeing compliance with privacy and data protection law in Belgium. Since 1 January 2004, the Privacy Commission has been an independent supervisory authority under the auspices of the Belgian House of Representatives. The Privacy Commission consists of 16 members, who are appointed for a renewable six-year mandate. The Privacy Commission's powers include:

- issuing opinions and recommendations on any matters relating to the application of the fundamental principles of data protection, on its own initiative or at the request of the different governments and legislators in Belgium;
- investigating privacy and data protection related complaints. In this respect, the Privacy Commission mainly plays a mediating role. If an amicable settlement cannot be reached, the Privacy Commission can issue an opinion on the legitimacy of the complaints, as well as specific recommendations directed to the controller;
- organising on-site investigations into potential privacy and data protection violations. For that purpose, members of the Privacy Commission have the status of assistant officers of the Public Prosecutor, and they have access to all places that may reasonably be linked to activities covered by the Data Protection Act. They can demand, among other things, the disclosure of any documents that may be of use for their investigation; and
- receiving and keeping a record of notifications submitted by controllers (or their local representatives) with regard to wholly or partly automatic data processing operations carried out in Belgium.

The Privacy Commission itself cannot impose sanctions for privacy or data protection violations. Instead, it must inform the Public Prosecutor of such violations, and the Public Prosecutor can subsequently decide whether or not to press charges. However, in some cases the President of the Privacy Commission may submit privacy and data protection disputes to the Court of First Instance.

3 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 civil or criminal penalties if the Privacy Commission decides to bring the case before the Court of First Instance or to refer it to the Public Prosecutor. Unlawful processing of PII is punishable with fines up to €600,000, confiscation of the media containing the PII, erasure of the data or a prohibition to manage any PII processing for a period of up to two years. The Belgian courts may also order the publication of their judgments in one or more newspapers. Any repeated violation of the Data Protection Act is punishable by a term of imprisonment of up to two years or fines of up to €600,000. In addition, violations of Belgian privacy and data protection law may result in civil action for damages.

Scope

4 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 is intended to cover all sectors and all types of organisations, but the following types of PII processing fall (partly) outside of its scope:

- 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;
- processing of PII solely for journalism purposes, or purposes of artistic or literary expression, if the processing relates to PII made public by the data subject or closely related to the public nature of the data subject or the facts in which the data subject is involved;
- processing of PII by the State Security Service, or the General Intelligence and Security Service of the Armed Forces;
- processing of PII managed by public authorities with a view to the fulfilment of their judicial police duties;
- processing of PII that is necessary to comply with anti-money laundering laws; and
- processing of PII managed by the European Centre for Missing and Sexually Exploited Children.

5 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 generally applies to interception of communications, electronic marketing or 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 2 July 2008 regarding the registration 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 Collective Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance at the workplace (surveillance of individuals).

6 Other laws

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

The following legislation also contains data protection rules:

- The Belgian 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).

7 PII formats

What forms of PII are covered by the law?

The Data Protection Act applies to the processing of PII wholly or partly by automatic means, and to the processing otherwise than by automatic means of PII that forms part of a filing system (or is intended to form part of a filing system). 'Filing system' refers to any structured set of PII that is accessible according to specific criteria, whether centralised, de-centralised or dispersed on a functional or geographical basis.

8 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 applies to processing of PII by a controller who is either established in Belgium (provided that the processing of PII is carried out in the context of the activities of the establishment) or not established in Belgium or another EU country, but who uses 'means' located on Belgian territory to process PII other than for transit purposes. 'Means' can refer to, for example, the use of service providers operating in Belgium.

9 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?

In principle, all types of PII processing fall within the ambit of the Data Protection Act, regardless of who is 'controlling' the processing or merely processing PII on behalf of a controller. The 'controller' is any natural or legal person, un-associated organisation or public authority that alone or jointly with others determines the purposes and means of the processing of PII. The obligations set forth in the Data Protection Act are mainly addressed to the controller. The concept of 'processor' refers to any natural person, legal person, un-associated organisation or public authority that processes PII on behalf of the controller, except for the persons who, under the direct authority of the controller, are authorised to process the data (eg, employees of the controller). Except for legal information security requirements, data protection obligations are imposed on processors through their mandatory contract with the controller.

Legitimate processing of PII

10 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 Data Protection Act includes the following, exhaustive list of potential legal grounds for processing of PII:

- the individual (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 an obligation to which the controller is subject under or by virtue of an act, decree or ordinance;
- the processing is necessary in order to protect the vital interests of the data subject;
- 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 in a third party to whom the PII is disclosed; or
- the processing is necessary for the legitimate interests of the controller (or the third party to whom the data 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 basis apply (see question 11).

11 Legitimate processing – types of PII

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

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

- the data subject has given his or her written consent to such processing;
- the processing is necessary to carry out the specific obligations and rights of the controller in the employment 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, health insurance 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;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for the purposes of scientific research (subject to certain conditions);
- the processing is necessary to comply with social security laws;
- the processing is carried out in accordance with the Act of 4 July 1962 on Public Statistics;
- the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment to the data subject or one of his or her relatives, or the management of healthcare services in the interest of the data subject, provided that the PII is processed under the supervision of a health professional;
- the processing is carried out by an association with legal personality or an organisation of public interest whose main objective is the protection and promotion of human rights and fundamental freedoms; or
- the processing of PII is authorised (by an act, decree or ordinance) for another reason of substantial public interest.

The processing of health-related PII is prohibited in principle, and can only be carried out if:

- the data subject has given his or her written consent to such processing;
- the processing is necessary to carry out the specific obligations and rights of the controller in the employment law area;
- the processing is necessary to comply with social security laws;
- the processing is necessary for the promotion and protection of public health, including medical examination of the population;
- the processing is required (by an act, decree or ordinance) for reasons of substantial public interest;
- the processing is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving his or her consent;
- the processing is necessary for the prevention of imminent danger or the mitigation of a specific criminal offence;
- the processing relates to PII that has been made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment to the data subject or to one of his or her relatives, or the management of healthcare services in the interest of the data subject, provided that the PII is processed under the supervision of a health professional; or
- the processing is required for the purposes of scientific research (and carried out under certain conditions).

The processing of litigation-related PII (including PII relating to suspicions, prosecutions or convictions in criminal matters or administrative sanctions) is prohibited in principle and can only be carried out if the PII is processed:

- under the supervision of a public authority or ministerial civil servant, provided the processing is necessary for the fulfilment of their duties;
- by other persons, if the processing is necessary to achieve purposes that have been established by law;
- by natural persons, private or public legal persons, to the extent that the processing is necessary to manage their own litigations;
- by lawyers or other legal advisors, to the extent that the processing is necessary for the protection of their clients' interests; or
- because the processing is required for scientific research and carried out under specific conditions established by law.

Data handling responsibilities of owners of PII

12 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 is processed. The Data Protection Act lists the information that must be provided to data subjects. If PII is obtained directly from the data subject, the controller (or its representative) must provide at least the following information no later than the moment the PII is obtained:

- the name and address of the controller (and of its representative, if any);
- the purposes of the processing;
- 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;
- whether it is compulsory to reply to requests for information and what the possible consequences of the failure to reply are;
- the existence of the right to access and rectify his or her PII; and
- other information dependent on the specific nature of the processing as specified by law (additional notice obligations apply, eg, when processing health data).

If PII is not obtained directly from the data subject, the controller (or its representative) must provide, in addition to the information listed above, the categories of PII concerned. This information must be provided when collecting PII or, when PII is shared with a third party, at the very latest when the PII is first disclosed.

13 Exemption from notification

When is notice not required?

Notice is not required if data subjects have already received the information mentioned in question 12. 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 statistical, historical or scientific research, or for the purpose of medical examination of the population with a view to protecting and promoting public health; or
- PII is recorded or provided to comply with legal provisions.

14 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 Protection Act 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 communication of the PII in an intelligible form;
- obtain, free of charge, the rectification of incorrect PII relating to them;
- object to the processing of their PII, for substantial and legitimate reasons related to their particular situation, unless the processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract with the data subject or when the processing is necessary for compliance with a legal obligation;
- obtain, free of charge, the erasure of or the prohibition to use PII relating to them that is incomplete or irrelevant with a view to the purpose of the processing or where the recording, disclosure or storage of the PII is prohibited, or where it has been stored for longer than the authorised period of time;
- object to the intended processing of their PII, free of charge and without reason, if PII is obtained for direct marketing purposes;
- complain to the Privacy Commission, free of charge, and request that the Privacy Commission exercises their rights on their behalf;
- not be subject to decisions having legal effects or significantly affecting them, which are taken purely on the basis of automatic data processing aimed at assessing certain aspects of their personality, unless the decision is taken in the context of an agreement or if it is based on a legal provision; and
- receive compensation from controllers for damage incurred as a result of a violation of the Data Protection Act, unless the controllers can prove that the facts that caused the damage cannot be ascribed to them.

15 Data accuracy

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

Under the Data Protection Act, controllers must ensure that the PII they collect and further process is adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed. Furthermore, PII must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that PII that is inaccurate or incomplete, with respect to the purposes for which it is collected or for which it is further processed, is erased or rectified.

16 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 processing purposes. Pursuant to the data minimisation principle, PII collected and processed must be proportionate to the processing purposes. In terms of data retention requirements, PII must be kept in a form that allows for the identification of data subjects for no 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.

17 Finality principle

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

The Data Protection Act 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. In its guidance concerning the registration of processing activities (see question 23), the Privacy Commission has identified a list of purposes that are considered legitimate.

18 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 as long as these are not incompatible with the initial purposes for which the PII was collected, taking into account all relevant factors, especially the reasonable expectations of the data subject and any applicable legal and regulatory provisions. Under specific conditions established by the Royal Decree, further processing of PII for historical, statistical or scientific purposes is not considered incompatible.

Security

19 Security obligations

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

Controllers and their processors are required to implement appropriate technical and organisational measures to protect PII from accidental or unauthorised destruction, accidental loss, as well as from alteration, access and any other unauthorised processing. These measures must ensure an appropriate level of security taking into account the state of technological development in this field and the cost of implementing the measures on the one hand, and the nature of the PII to be protected and the potential risks related to the processing on the other hand. The more sensitive the PII and the higher the risks for the data subject are, the more precautions have to be taken. For example, the processing of health-related PII outside a medical context (eg, by a life insurance company) should be subject to stricter security measures.

In 2013, the Privacy Commission issued non-binding guidance by means of a 'Recommendation' on information security and, in particular, working with computer files. The Recommendation supplements and builds on two previously issued guidance documents from the Privacy Commission: the 2012 Reference Measures for the Security of Any Personal Data Processing Operation and the 2012 Guidelines Relating to Information Security of Personal Data. Jointly, these three guidance documents are intended to assist controllers and processors in their efforts to implement suitable security measures in compliance with the Data Protection Act.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and 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 Privacy Commission. 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 Privacy Commission 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.

Except for the notification duty in the Electronic Communications Act, there is currently no general breach notification obligation. However, the Privacy Commission strongly recommends all types of controllers to notify security breaches. It has published a separate template form on its website to be used by controllers other than providers of electronic communication services for purposes of notifying security breaches. The Privacy Commission expects controllers to report a breach incident within 48 hours of discovery and, in some cases, to notify affected individuals as well. Failure to notify in the event of a security incident could trigger liability under Belgian data protection law. Upon notification, the Privacy Commission will generally conduct a formal investigation into the security incident, and examine how PII was processed and protected prior to the incident.

Although the Privacy Commission has taken the position that notifying security incidents is strongly recommended, the Privacy Commission acknowledges that notification is not necessary if: it is clear from the circumstances that the incident will not affect the privacy or PII of the individuals concerned; the controller can demonstrate that the PII was encrypted or otherwise protected so that the PII is not 'useful' in the hands of third parties; or affected individuals have been informed immediately of the scope and consequences of the security incident, provided that only a limited number of individuals were affected (not more than 100) and no 'sensitive' PII (eg, health-related PII) was involved.

Internal controls

21 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 except in limited cases where a prior authorisation of the Privacy Commission is required for the data processing activity (eg, for processing PII from certain government databases).

Nevertheless, the Privacy Commission recommends controllers to appoint a person responsible for the implementation of the organisation's information security policy (a data protection officer) where the nature of the personal data processed justifies such information security measure. The main task of the data protection officer is to ensure that the various responsibilities with regard to information security (prevention, supervision, detection and processing) have been clearly defined and that the persons in charge of information security within the organisation can operate autonomously and independently.

22 Record keeping

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

The Data Protection Act does not provide any explicit obligations to maintain internal records or establish internal processes or documentation, unless sensitive PII is processed. In the latter case, the controller or processor must keep a list of categories of individuals having access to such PII with a precise description of their function with respect to the data processing activity. This list should be available to the Privacy Commission.

Furthermore, the Privacy Commission's recommendations on information security provide that controllers should have complete and centralised documentation relating to information security within their organisation, which is updated on a regular basis and contains at least the following information:

- the identity of the data protection officer (if any);
- an information security policy;
- an overview of the implemented security measures;
- an inventory of the PII being processed, its location and the operations performed on it;
- a list with the names of the bodies or designated individuals having access to the PII;

- a description of the system and network configuration;
- technical documentation about the security controls that are implemented;
- a schedule of planned operations;
- an intrusion detection policy;
- security control test plans;
- incident reports; and
- audit reports, if any.

Registration and notification

23 Registration

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

As a general rule, controllers (as opposed to processors) are required to register their data processing activities with the Privacy Commission. A number of data processing activities are, however, exempted from the general registration obligation provided that certain conditions are met. For example, PII processing for the following purposes may not require registration: payroll management, employee administration, accounting, administration of shareholders and partners, customer and supplier management, communication purposes and access control. Furthermore, exemptions to the general registration obligation exist for certain data processing activities of non-profit organisations, educational organisations and public authorities.

24 Formalities

What are the formalities for registration?

Controllers can register their data processing activities by completing an online registration form on the Privacy Commission's website or by submitting a paper registration form (which can be downloaded from the Privacy Commission's website).

The following information needs to be provided in the registration form:

- identification details of the controller (such as name, corporate address, legal form, etc);
- name of the data processing;
- purposes of the data processing;
- categories of PII processed;
- legal basis for the data processing;
- categories of data recipients and measures implemented to secure the disclosure of PII to these data recipients;
- means of informing the data subjects about the processing of their PII;
- a person or department that data subjects can contact to exercise their rights and measures implemented by the controller to facilitate data subjects in exercising their rights;
- retention period of each category of PII;
- description of the information security measures implemented by the controller;
- international data transfers (including legal basis – eg, EU Model Contracts – for international data transfers to non-adequate countries outside the EU); and
- details of the contact person and signatory of the registration form.

After submitting the registration form, the controller is required to pay a registration fee of €25 for online registrations or €125 for paper registrations.

Registrations do not need to be renewed periodically, but they must be updated if their content is no longer accurate.

25 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 complying with the registration obligation may lead to criminal fines ranging between €600 and €600,000. In case of recidivism, the controller may, in addition to a fine, be convicted to imprisonment of up to two years. The courts can also order the publication of their judgment in one or more newspapers, the confiscation of data storage media and the erasure of PII. In addition, the courts can prohibit the convicted person from managing any processing of PII for a period of up to two years.

26 Refusal of registration

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

The Privacy Commission may refuse a registration if the information provided in the registration form is not complete or the registration fee has not been paid.

27 Public access

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

A public register is available online on the Privacy Commission's website (https://eloket.privacycommission.be/elg/searchPR.htm?eraseResults=true&siteLanguage=nl). This register is also available at the offices of the Privacy Commission and individuals can request an extract from the public register by letter.

28 Effect of registration

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

Controllers may initiate their PII processing activities as soon as the required registrations have been completed. Registrations as such do not exempt a controller from any of its other obligations under the Data Protection Act. Controllers need to ensure that their processing activities are in line with the submitted registrations (eg, only process PII for the purposes identified in the registration) and should inform the Privacy Commission of any changes to the registered processing activities.

Transfer and disclosure of PII

29 Transfer of PII

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

When a controller outsources data processing activities to a third party (ie, the processor), it should put in place a (written or electronic) agreement with the processor that specifies:

- the technical and organisational information security measures to be implemented by the processor;
- the processor's liability towards the controller; and
- the processor's obligation to only process the PII in accordance with the controller's instructions.

30 Restrictions on disclosure

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

In general, there are no specific restrictions on the disclosure of PII other than the restrictions resulting from the general data protection principles (such as notice and purpose limitation). Health-related PII can, however, only be disclosed to health professionals (and their agents and assignees) bound by a secrecy obligation, unless the data subject has given his or her written consent for the disclosure or if the disclosure is necessary to prevent an imminent danger or to suppress a specific criminal offence. Furthermore, data subjects may submit a request to the President of the Court of First Instance to issue an injunction prohibiting the disclosure of PII.

31 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 unambiguously given his or her consent to the proposed transfer;
- 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;

Update and trends

In 2015 the Privacy Commission undertook a number of initiatives related to the protection of individuals' privacy in an online context (such as issuing an opinion on the use of cookies and participating in the Internet Sweep Day organised by the Global Privacy Enforcement Network). Other topics on the Privacy Commission's agenda included the legislation around drones, anti-terrorism measures proposed by the federal government, issues related to cloud computing and employee privacy matters.

The Privacy Commission will now most likely start preparing for its new role under the EU General Data Protection Regulation, which enters into force in May 2018. Furthermore, international data transfers and the mechanisms available to companies to legitimise such transfers will most likely also remain a high priority on the Privacy Commission's agenda for the coming year.

- 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 or legally required in light of the 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
- the transfer is made from a register that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

In addition to the exemptions listed above, cross-border transfers to non-adequate countries can be authorised by the Minister of Justice (via Royal Decree) 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 a data transfer agreement or implementation of Binding Corporate Rules. Prior authorisation by the Minister of Justice is, however, not required if the controller has executed the 'Standard Contractual Clauses' approved by the European Commission.

32 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 Privacy Commission. However, if the controller is required to register its data processing activities with the Privacy Commission, any cross-border data transfers, as well as the legal grounds for transfers to countries not providing an adequate level of data protection, must be indicated in the registration.

As mentioned in question 31, prior authorisation by the Minister of Justice is required if the controller relies on Binding Corporate Rules or 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. In the latter case, a copy of the executed Standard Contractual Clauses must be submitted to the Privacy Commission for review.

33 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 31 and 32 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, unless the PII is transferred on the basis of the Standard Contractual Clauses (which contain specific requirements for onward data transfers).

Rights of individuals

34 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 (by sending a signed and dated access request together with proof of his or her identity), 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 nature and origin of the PII processed;
- the categories of individuals to whom his or her PII is or has been provided;
- the logic involved in any automated decision making (if any); and
- the existence of the right to object to the processing or request rectification or deleting of his or her PII, as well as the possibility to initiate a proceeding before the President of the Court of First Instance and to consult the public register of the Privacy Commission.

The controller should also provide the PII to the data subject in an intelligible form. This does not necessarily imply that the data subject is entitled to receive a copy of his or her PII or to have direct access to the file that contains his or her PII. Controllers can freely choose how they provide this information to the data subject.

Limitations to the right of access exist for PII processed:

- by certain public authorities, including police services and tax authorities;
- in the context of the application of anti-money laundering legislation;
- for journalistic, artistic or literary purposes, where providing access would compromise the intended publication or reveal information sources;
- in the medical file of a patient; and
- in the context of medical scientific research.

35 Other rights

Do individuals have other substantive rights?

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

Correction and deletion

Data subjects are entitled to obtain, free of charge, the rectification of incorrect PII relating to them. Furthermore, data subjects have the right to request the erasure of or the prohibition to use all PII that is incomplete or irrelevant with a view to the purpose of the processing, or where the recording, disclosure or storage of the PII is prohibited, or where it has been stored for longer than the authorised period of time.

Objection to processing

Individuals have the right to object to the processing of their PII for substantial and legitimate reasons related to their particular situation, unless 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, or compliance with a legal obligation to which the controller is subject. Data subjects are in any event (ie, without any specific justification) entitled to object to the processing of their PII for direct marketing purposes.

Complaint to relevant supervisory authorities and enforce rights in court

Data subjects are entitled to request the Privacy Commission to exercise their rights on their behalf. Furthermore, they 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, which are taken purely on the basis of automatic data processing aimed at assessing certain aspects of their personality, unless the decision is taken in the context of an agreement or if it is based on a legal provision.

36 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 damages (including injury to feelings) as a result of a violation of the Data Protection Act. Controllers will only be exempt from liability under the Data Protection Act if they are able to prove that the facts that caused the damage cannot be ascribed to them.

37 Enforcement

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

The Privacy Commission can act as mediator between data subjects and controllers, and can address recommendations to controllers (with a view to ensuring the latter's compliance with the Data Protection Act), but it has no actual enforcement power. Enforcement of data subjects' rights is only possible through legal action before the courts.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

No.

Supervision

39 Judicial review

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

Controllers cannot appeal against the decisions of the Privacy Commission, as these are not legally binding.

Specific data processing

40 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 strictly necessary to provide a service explicitly requested by the individual.

On 4 February 2015, the Privacy Commission 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.

41 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.

HUNTON& WILLIAMS

Wim Nauwelaerts **wnauwelaerts@hunton.com**
David Dumont **ddumont@hunton.com**

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

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

42 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 Privacy Commission 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 the Data Protection Act when relying on providers of cloud computing services.

Some of the risks identified by the Privacy Commission include:

- loss of control over the data due to physical fragmentation;
- increased risk for 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 cloud provider's business or the service contract; and
- violations of data transfer restrictions.

To address these risks, the Privacy Commission has issued a number of guidelines for data controllers that want to migrate data to a cloud environment. The Privacy Commission 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

Ricardo Barretto Ferreira and Paulo Brancher

Azevedo Sette 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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Although there are several rules related to data privacy in Brazil, so far there has been no consolidation of all the applicable rules into a single law. The Brazilian Federal Constitution states that the privacy, private life, honour and image of persons are inviolable, and that the right to compensation for economic and non-economic damages resulting from violation thereof is guaranteed. It also states that the confidentiality of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, upon court order, in the event of, and in the manner established by law for, purposes of criminal investigation or criminal procedural discovery.

Moreover, the Brazilian Internet Bill of Rights (Law 12,965/2014) (the Internet Law) and Resolution 3/2009 of the Internet Steering Committee in Brazil (www.cgi.br) establish principles for ensuring privacy and data protection. Under the Internet Law, any collection, use, storage or processing of personal data through the internet is subject to the users' express consent and must be limited to the purposes that justified it. The recently enacted Decree 8,771 of 11 May 2016, which regulates the Internet Law, establishes rules on the request of registration data by public administration authorities, as well as on the security and confidentiality of records, personal data and private communications.

In addition to constitutional protection, privacy and data protection are mentioned in specific and different laws, including, but not limited to, the Consumer Protection Code (Law 8,078/1990), the Civil Code (Law 10,406/2002), the Law on Public and Private Archives and the Bank Secrecy Law (Complementary Law 105/2001).

There is an important bill of law (PL 5,276/2016) for personal data protection and privacy in progress in the Brazilian Congress that is intended to meet the OECD guidelines and the European Union's data protection standards. This bill of law has received all sorts of suggestions and comments by the civil society and gone through discussions in various Commissions of the Brazilian Congress for a long time already. There is no expectation as to when this process will be finished.

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 authority in charge of data protection in Brazil, although the Decree 8,771/2016 provides that supervision and verification of infringements of its rules (including data protection rules) will be conducted in a tripartite manner. The National Telecommunications Agency (Anatel) will act under Law 9,742/1997 (Telecommunications Law), the Consumer General Secretariat, subordinated to the Ministry of Justice, will act in relation to the Consumer Protection Code, and the Administrative Council for Economic Defense (CADE), will do it in case of violations against the economic order. Such bodies, as well as other bodies and entities of the federal public administration, will act in a collaborative manner following the guidelines fixed by the Internet Steering Committee (www.cgi.br).

3 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 Internet Law, without prejudice to other civil, criminal or administrative provisions, provides that any breach of data protection or privacy regarding the collection, storage, custody and treatment of records, personal data or communications by internet connection or applications providers will be subject, as applicable, to the following sanctions, that may be applied on an individual or cumulative basis:

- warning for a corrective action;
- a fine of up to 10 per cent of the revenues of the economic group in Brazil in its most recent financial year;
- temporary suspension of its activities; and
- prohibition of certain activities.

The disclosure of proprietary information can also be classified as a crime of secret disclosure or violation of professional secrecy, or both, with a penalty of detention or a fine, or both. Law 12,737/2012, which provides for cybercrime, also establishes a penalty of three months' to one year's detention and a fine for those who break into a third-party computer device to obtain or destroy data or information without the express or implied consent of the corresponding owner.

The Brazilian Consumer Protection Code determines a penalty of imprisonment or fine, or both, to those who block or hinder access by the consumer to information about him or her contained in files, databases or records, or those who are expected to know that information relating to the consumer as contained in any file, database, record or registration is incorrect and, nevertheless, fail to immediately rectify it. The same statute sets forth administrative penalties imposed by the authorities in charge of protecting consumer rights, and such penalties include fines, intervention and counter-advertising.

The Bank Secrecy Law (Complementary Law 105/2001) establishes a penalty of imprisonment and a fine for financial institutions (and similar entities) that breach the secrecy of the financial operations of, and the financial services provided to, its users.

Scope

4 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 mentioned below, so far Brazil has no consolidated and specific law regarding data protection. General principles and rules such as the Federal Constitution, the Internet Law, the Civil Code and the Consumer Protection Code apply to all Brazilian citizens. Moreover, there are special provisions that apply only to certain sectors and areas of activity.

5 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 Brazilian Federal Constitution ensures the secrecy of correspondence, telegraphic, data and telephone communications, except upon court order, in the cases provided for in the law for the purposes of criminal investigation or procedure.

6 Other laws

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

Some of the specific data protection rules applicable to special sectors and areas of activity are listed below:

- the Internet Law (Law 12,965/2014), Decree 8,771/2016 and Resolution 3/2009 of the Internet Steering Committee in Brazil (www.cgi.br) establish principles and rules for ensuring privacy and data protection in the use of internet in Brazil, mainly regarding the activities developed by the internet service providers;
- the Consumer Defence Code (Law 8,078/1990) provides for several rights of consumers as regards personal information in 'consumer databases and reference files', such as the right to access and modify or correct their data, wherever they are, and the right to ask for and obtain the deletion of such data;
- the Positive Credit Registry Law (Law 12,414/2011) permits the collection of 'positive' credit information (ie, fulfilment of contracted obligations) but prohibits the register of excessive information (ie, personal data which is not necessary for analysing the credit risk) and sensitive data;
- the Brazilian Telecommunications Law (Law 9,472 1997) grants privacy rights to consumers in relation to the telecommunications services;
- the Bank Secrecy Law (Complementary Law 105/2001) requires that financial institutions (and similar entities) hold financial data of individuals and entities in secrecy, except under judicial order issued for purposes of investigation of any illegal acts or criminal procedural discovery;
- the Civil Code (Law 10,406/2002) grants general privacy rights to any individual and the right to claim against any attempt to breach such rights by any third party; and
- Resolution 124/2006 of the National Supplementary Health Agency imposes a fine on healthcare insurance companies of up to 50,000 reais for the breach of personal information related to the health conditions of a patient.

7 PII formats

What forms of PII are covered by the law?

There are no restrictions on the scope of protection for private information.

8 Extraterritoriality

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

No. Brazilian law shall apply to all cases where PII belongs to a Brazilian individual. Moreover, the Internet Law sets forth that any process of collection, storage, custody and treatment of records, personal data or communications by connection and applications service providers, in which at least one of these acts occurs in the national territory, shall comply with Brazilian law and regulations regarding rights to privacy, confidentiality of personal data and secrecy of private communications and records. The aforementioned provision applies even if the activities are carried out by a legal person located abroad, as long as the services are offered to the Brazilian public or at least one member of the same economic group owns establishments in Brazil.

9 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?

As a general rule, all processing or use of PII is covered by the Brazilian privacy and data protection laws and regulations. However, considering that so far there is no consolidated and specific law regarding the matter, the situation shall be verified on a case-by-case basis under Brazilian law.

Legitimate processing of PII

10 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 rule under Brazilian law is the need for express consent of the individual regarding the use and processing of their PII. Also, the Internet Law assures internet users of:

- express consent on the collection, use, storage and processing of personal data, which should occur irrespective of the other contractual terms; and
- clear and complete information on the collection, use, storage, treatment and protection of their personal data, which can only be used for purposes that justify their collection, are not forbidden and are specified in the service agreement or terms of use.

11 Legitimate processing – types of PII

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

Brazilian law does not make express distinction between personal and sensitive data. Nevertheless, information regarding religion, sexual orientation, political position, health, etc, can be construed as sensitive data, and its improper use or collection can be deemed to be a crime depending on the case (eg, racism, discrimination).

According to the Brazilian Consumer Protection Code, consumer-related databases must not contain negative information for a period exceeding five years.

See question 6.

Data handling responsibilities of owners of PII

12 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 specific circumstances, notification may be required under Brazilian law. The Consumer Protection Code, for instance, imposes a notification in writing to the consumer for the opening of a file, record or any personal or consumer data, in cases where such record has not been requested by the consumer.

13 Exemption from notification

When is notice not required?

In particular cases, personal data may be disclosed by service providers if so required by a court order and according to the law, without notice to the corresponding individual. In these cases, the judge will be responsible for taking the necessary measures to ensure confidentiality of the information received and to safeguard the privacy, private life, honour and image of the user.

14 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 already mentioned, as a general rule, the collection and use of personal data requires prior, clear and express consent of the individual. Also, the Federal Constitution assures Brazilians and foreign nationals the right to rectify their data, and the Consumer Protection Code provides that

individuals have the right to access all data stored about themselves, and request changes, corrections and even removal from a certain database.

Taking into consideration that consumers and employees are construed as the weaker party of a relationship under the Brazilian framework, the collection and use of their PII require a more careful degree of control.

15 Data accuracy

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

As a general rule, the PII collected or stored must be objective, necessary and accurate, otherwise the individual may demand immediate correction or exclusion of such data from the databases and also request compensation for damages.

16 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?

According to the Brazilian Consumer Protection Code, consumer-related databases must not contain negative information about a consumer for a period exceeding five years.

Moreover, the Internet Law establishes that 'application service providers' (incorporated as legal entities, and that exercise their activities in an organised manner, professionally and with economic purposes) must keep records of access to internet applications (ie, the set of information regarding date and time of use of a particular internet application from a particular IP address) under secrecy, in a controlled and safe environment, for a minimum term of six months, in accordance with the regulation (not enacted yet). In the provision of internet connections, it is incumbent on the autonomous system administrator to keep records of the connection logs (the set of information regarding the initial and final date and time of internet connection, its duration and the IP address used by the terminal for sending and receiving data packets) under the same conditions, but for at least one year. Both periods may be extended upon the request of the police, administrative authority or public prosecutors.

17 Finality principle

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

The Internet Law grants individuals the right to have clear and complete information about the collection, use, storage, processing and protection of their personal data, which can only be used for purposes that justify their collection, are legal and are provided for in the corresponding service agreement. The law also forbids the custody of PII that may be construed as excessive considering the initial purposes for which consent was given.

In addition, Decree 8,771/2016 provides that administrative authorities must request registration data with specification of the data owners stating the legal grounds of their express competence and the reason for access thereof, any non-specific request being forbidden. Moreover, public federal administration bodies are required to adopt transparency measures and publish statistical reports on registration data requests.

The Consumer Protection Code follows the same principles: the collection and processing of personal data are justifiable depending on the services to be provided.

18 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?

All use of PII should be clearly communicated and authorised by any individual whose data will be collected or stored, or both. In this regard, it is worth mentioning that a Brazilian telecommunications company was fined 3.5 million reais by the Department of Consumer Protection of the Brazilian Ministry of Justice for abusive practices against consumers under the Brazilian Protection Code, and breach of good faith and privacy because it collected, monitored, used and redirected data traffic from internet users for business purposes and without the appropriate and express consent from such consumers.

Security

19 Security obligations

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

The Internet Law brings a few security requirements, which are specifically provided by Decree 8,771/2016. Internet service providers must follow guidelines for security standards in the handling of personal data and private communications, such as:

- definition of responsibilities and authentication mechanisms so as to ensure individualisation of the persons who will have access to and handle data, as well as create detailed access logs;
- creation of detailed inventory of access to connection records and access to applications containing time, duration, identity of the designated employee or responsible for the access in the company and the accessed file; and
- the management solutions of records through techniques that ensure the inviolability of data, such as the use of encryption. The safeguard and availability of connection logs and access data, as well as PII and the content of private communications, must meet the requirements of preservation of intimacy, privacy and image of the parties directly or indirectly involved.

20 Notification of data breach

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

There is no specific provision that requires notification to the regulator or individuals in the case of security breaches. However, considering the finality principle, and all other rights granted to those individuals whose data are being collected, it is assumed and expected that any security breaches that may harm those rights will lead to the individuals being informed. In that way, individuals may take actions to maintain the privacy of their personal data or information, without extinguishing the provider's liability for any damages arising from such security breach.

Internal controls

21 Data protection officer

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

There is no specific regulation on this matter in Brazil.

22 Record keeping

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

The internal processes required are the ones already mentioned, regarding safety and transparency of activities. All individuals must know which data are being collected, where and how they are being stored and what they are used for.

Registration and notification

23 Registration

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

As per our answer to question 2, so far there is no authority in charge of data protection in Brazil.

24 Formalities

What are the formalities for registration?

No specific registration is required for owners and processors of PII under Brazilian law in addition to the formalities needed for the exercise of a company's activities in Brazil.

Update and trends

The Brazilian law currently in force does not provide legal certainty on the processing of personal data by private entities. The Internet Law is a great step towards data protection and privacy in the internet environment; however, it does not assure privacy and data protection as a whole. This is principally because it is applied only to internet connection providers and internet application providers, and does not encompass several important issues such as the processing of sensitive data, interconnection and transfer of personal data. The bill of law aims to solve this lack of legal certainty.

According to the bill of law, personal data processing activities shall comply with several principles, such as purpose, transparency, security, free access by the data subject, prevention of damages and non-discrimination.

Consent is the key issue to legitimate personal data processing. The bill of law expressly provides that personal data processing is only allowed under free, express, specific and informed consent. This means that generic consent for personal data processing shall be invalid and anyone that obtains personal data by error, fraud, state of need or coercion is subject to penalties.

The bill of law also establishes special rules on sensitive personal data processing, which can only take place under special consent, or without consent in certain circumstances, such as the fulfilment of legal obligation.

International transfer is only allowed by the bill of law for countries that provide a level of protection for personal data that is equivalent to the level established in the Brazilian law. If personal data is transferred to a country that does not provide an adequate level of protection, special consent is required.

Security measures and good practices are also required by the bill of law, and private legal persons shall be subject to administrative penalties for any breaches of the standards established in the law, which may be applied by a regulatory agency created by the Brazilian government.

In view of this, despite the fact that there is no expectation as to when the bill of law will be approved, Brazilian and foreign companies that process personal data have attempted to implement policies on privacy and personal data protection, and ultimately maintain transparent corporate governance.

25 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 24.

26 Refusal of registration

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

See question 24.

27 Public access

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

See question 24.

28 Effect of registration

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

See question 24.

Transfer and disclosure of PII

29 Transfer of PII

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

The Brazilian legal framework does not contain specific rules regarding the transfer of PII to outsourced processing services. All the aforementioned Brazilian principles, rules and limitations also apply in this case and therefore the express consent of the individual for the collection, transfer and use of its PII is needed.

It is worth mentioning that the Internet Law does not allow for the connection service providers' liability for retaining connection logs being transferred to third parties.

30 Restrictions on disclosure

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

See question 29.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

As a general rule, the transfer of PII outside the jurisdiction is not forbidden but Brazilian law must be observed.

In this regard, the Internet Law establishes that the Brazilian law and the regulations regarding rights to privacy, confidentiality of personal data and private communications and records apply even if the internet service providers' activities are carried out by a legal person located abroad, as long as the services are offered to the Brazilian public, or at least one member of the service providers' economic group owns establishments in Brazil.

32 Notification of cross-border transfer

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

There is no specific authority in charge of data protection in Brazil.

33 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 is no specific law in this regard in Brazil; however, based on general principles of law, such transfers cannot impair the applicability of the Brazilian rules or regulations, if such rules or regulations are applicable to such specific PII.

Rights of individuals

34 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 mentioned in question 14, the Federal Constitution assures Brazilian and foreign nationals the right to rectify their data.

In addition, the Consumer Protection Code provides that individuals have the right to access all data stored about themselves and request changes, corrections and even its removal from a database. Preventing or hindering a consumer's access to information about him or her, or failing to immediately correct inaccurate information, shall subject the person responsible to detention of up to one year or a fine, or both, and also compensation for damages arising from such inaccuracy.

35 Other rights

Do individuals have other substantive rights?

See question 34.

36 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 who have their PII violated are entitled to pain and suffering and property damages by filing a suit before the Brazilian courts. In this regard, the Brazilian Superior Court of Justice reached a consensus that petitioners are not required to provide evidence of pain and suffering as a result of violation of their privacy, since 'harm is presumed upon violation

of such protected legal interest'. On the other hand, property damages – such as incidental damages and loss of profit – require proof that such damages actually occurred.

37 Enforcement

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

Individuals who have their PII violated are entitled to claim their rights before the Brazilian courts, and, depending on the situation in which the violation occurred, individuals may also be entitled to claim certain rights before the consumer protection departments and regulatory agencies as well.

Public prosecutors and authorised associations under the law may also file class actions in the case of extensive violation of collective ('diffuse') interests, including consumer and privacy violations. If such proceeding is successful, courts may impose significant indemnifications to be paid to specific public funds, in addition to any individual indemnifications paid to the individuals.

Exemptions, derogations and restrictions

38 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 further exemptions or restrictions.

Supervision

39 Judicial review

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

There is no specific authority in charge of data protection in Brazil. However, as a rule, administrative orders can be the subject matter of appeals to the Brazilian courts.

Specific data processing

40 Internet use

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

Taking into consideration that the use of 'cookies' is construed to be a monitoring tool, use should be subject to the individual's express consent.

41 Electronic communications marketing

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

There are no specific rules in this regard in Brazil, and the general principles and rules shall apply. The Brazilian Advertising Self-Regulatory Council reflects well the need to apply to advertisements on the Internet the same policy adopted for 'conventional' advertisements.

42 Cloud services

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

Cloud computing services have no specific regulation in Brazil. However, all principles and rules for data protection and cybersecurity are applied thereof.

Azevedo Sette
ADVOGADOS

Ricardo Barretto Ferreira **barretto@azevedosette.com.br**
Paulo Brancher **brancher@azevedosette.com.br**

Av. Pres. Juscelino Kubitschek, 2041
Torre E, 16º andar
04543-011, São Paulo
Brazil

Tel: +55 11 4083 7600
Fax: +55 11 4083 7601
www.azevedosette.com.br

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The legal framework for data protection can be found in article 19 No. 4 of the Political Constitution of the Republic of Chile that 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).

Chile has not formally adopted any international instrument on privacy or data protection.

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 upon a request of 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 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 45,000 to 450,000 Chilean pesos). Fines are viewed and determined in a summary procedure.

The Law establishes a general rule under which both non-monetary and monetary damages that result from wilful misconduct or negligence in the processing of personal data shall be compensated. In those cases, the amount of compensation shall be established reasonably by the civil judge, considering the circumstances of the case and the relevance of the facts.

Scope

4 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.

5 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
- article 222 to 226 of the Criminal Code of Procedure.

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).

6 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 economical, financial, banking or commercial character;
- Law No. 18,290, which contains provisions regarding the privacy of a driver's information; and
- Law No. 19,799 regarding electronic signatures, which contains the right of privacy of the holder of an electronic signature.

7 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.

8 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.

9 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?

Yes, all processing of PII is covered. 'Data processing' is 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, which has the authority to implement the decisions related to the processing of personal data.

Legitimate processing of PII

10 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 who the personal data refers to) 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;
- 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 they have been collected for, 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.

11 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 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 eventually 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.

Data handling responsibilities of owners of PII

12 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.

13 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.

14 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 are 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.

15 Data accuracy

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

Yes. The Law requires that the 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.

16 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 that relates 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.

17 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.

18 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 provisions. Purposes beyond the scope of the Law or the Chilean legal system are not allowed.

There are two exceptions to the aforesaid principle, and it comes when the data has been collected from sources available to the public and when the individual has given his or her express consent in the data processing.

Security

19 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.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and 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

21 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.

22 Record keeping

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

No, owners of PPI 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.

Registration and notification

23 Registration

Are PII owners and/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.

24 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.

25 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.

26 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.

27 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.

28 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.

Transfer and disclosure of PII

29 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 13.

30 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.

31 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.

32 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.

33 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 above-mentioned.

Rights of individuals

34 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 are 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 (goverment 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.

35 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 the 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.

Update and trends

The Chilean government is currently working on a bill that seeks to amend the current legislation on personal data, updating it and adapting it with the standard guidelines of the Organisation for Economic Co-operation and Development and EU Directive 95/46/EC. This bill should be sent to Congress in the second semester of 2016. The main aspects that the bill seeks to introduce into Chilean legislation are:

- providing some exceptions to the scope of the Law, namely, private family databases; databases for security, intelligence and defence; and databases ruled by special laws;
- the express recognition of the principles of consent, finality, proportionality, quality, transparency, responsibility and security;
- protection of different kinds of data, such as health-related data, telecom-related data, minors-related data, biometric data and commercial information-related data;
- detailed provisions about international transfer of personal data;
- creation of a national database record;
- creation of a national authority of personal data: a national council on data protection; and
- different kinds of fines or penalties for breach of the Law, according to the decree of the breach.

In general, the bill seeks to strengthen the current status of personal data in Chile, balancing the free flow of information and the rights of people. This bill has not yet been presented to the Congress.

36 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 3, 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.

37 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

38 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

39 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

40 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 it will require authorisation of the individual, unless there are exceptions contemplated by the Law, if not subject to the exceptions mentioned in question 13.

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

42 Cloud services

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

There are no rules or regulator 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 approximately between 45,000 and 450,000 Chilean pesos, 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 compensate.

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

Denmark

Michael Gorm Madsen
Lundgrens Law Firm P/S

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The Act on Processing of Personal Data (Act No. 429 of 31 May 2000 with subsequent amendments) (DPA) entered into force on 1 July 2000. The Act implements Directive 95/46/EC. The Act is supported by a number of statutory orders and guidelines and sector-specific regulation.

Denmark has incorporated 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.

The DPA is supervised by the Danish Data Protection Agency (the Agency). The Agency has the power to:

- act on its own initiative or on a complaint from a data subject;
- require to be furnished with any information of importance to its activities; and
- at any time, without any court order, have access to all premises from which processing operations are carried out by the public administration; or by private data controllers to the extent that such processing involves processing of sensitive PII or is carried out in connection with video surveillance.

3 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 may lead to criminal penalties, including imposition of fines or up to four months' imprisonment.

Criminal offences may be prosecuted by the Agency or by public prosecution by the police.

The most severe sanction for violation of the DPA so far imposed by the Agency is a fine in the amount of 25,000 kroner.

Furthermore, the Agency has the power to:

- order a private data controller to discontinue unlawful processing and to rectify, erase or block PII undergoing such processing;
- prohibit a private data controller from using a specific procedure if the Agency finds that the procedure in question involves a considerable risk that data are processed in violation of the DPA; and
- order a private data controller to implement specific technical and organisational security measures.

Scope

4 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 the public as well as to the private sector. However, exemptions apply for certain types of processing. Most significantly the DPA does not apply to the processing of data undertaken by an individual for purely personal and domestic purposes.

Further, the DPA does not apply to the processing of data that is performed on behalf of the Danish parliament and its related institutions, the intelligence services of the police and the national defence. The DPA applies only to a limited extent to processing for journalistic purposes and to the processing of data for the sole purpose of artistic or literary expression.

Provisions relating to information obligations to data subjects, and data subjects' rights to access data and certain other rights, are restricted in relation to processing of data by the courts, the police and the prosecution in criminal law matters.

5 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.

Such matters are generally covered by the DPA. Besides the DPA the following acts are relevant:

- the Marketing Practices Act (electronic marketing);
- the Act on Video Surveillance (monitoring and surveillance);
- the Criminal Act (interception of communications);
- the Act on Electronic Communications Network and Services (interception of communications); and
- the Executive Order on retention and storage of traffic data by providers of electronic communications networks and services (as amended due to the Court of Justice's ruling on Directive 2006/24/EC).

6 Other laws

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

Danish legislation includes many provisions dealing with data protection, some of which are included in the Archives Act, Act on the Civil Registration System, Act on Electronic Signatures, the Financial Business Act, the Payment Services Act, the Health Act, the Security Trading Act and the Public Administration Act, etc.

7 PII formats

What forms of PII are covered by the law?

The DPA applies to the processing of PII wholly or partly by electronic means, and to the non-electronic processing of PII in a filing system or PII intended to be included in a filing system, namely any structured set of PII accessible according to specific criteria, so that PII on a specific individual is readily accessible.

The DPA also applies to other non-electronic systematic processing of data for private data controllers and that includes data on individual persons' private or financial matters or other data on personal matters that can reasonably be claimed to be withheld from the public.

In addition, the DPA applies to any processing of PII in connection with video surveillance.

8 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 data controllers established in Denmark if the activities take place within the European Community.

A data controller is established in Denmark if the actual performance of activities is undertaken through a more permanent structure in Denmark. This may include activities carried out by a resident, a Danish incorporated company, branch, agency, office or other regular presence in Denmark.

The DPA also applies to data controllers established outside the European Economic Area (EEA) if:

- processing is carried out with the use of equipment situated in Denmark for purposes other than simple transit through the territory of the European Community; or
- if PII is collected in Denmark for the purpose of processing in a non-EEA country.

A third-country data controller subject to the DPA because the controller uses data processing equipment in Denmark must appoint a representative in Denmark and inform the Agency in writing of the identity of the representative.

9 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?

The DPA applies to all processing of PII; defined as any operation or set of operations performed upon PII, including, for example, collection, use, amending, storing, deleting and destruction.

The DPA distinguishes between data controller and data processor. The data controller determines the purposes and means of the processing of personal data, whereas the data processor is only processing the personal data on behalf of and under the instruction of the controller. The data processor is not directly subject to the requirements of the DPA except that the DPA requires data processors – as well as data controllers – to implement appropriate technical and organisational measures to prevent PII from being unlawfully processed.

Legitimate processing of PII

10 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 DPA sets out different grounds for legitimate processing depending on whether the PII is sensitive or non-sensitive. Non-sensitive PII is any PII not specifically defined by the DPA as sensitive or semi-sensitive (see question 11).

The main grounds for processing non-sensitive data are:

- the data subject has given his or her explicit and informed consent;
- it is necessary for the performance of a contract to which the data subject is party or in order to take pre-contractual steps at the request of the data subject;
- it is necessary for compliance with a legal obligation applicable to the controller;
- it is necessary in order to protect the vital interests of the data subject;
- it is necessary for the performance of a task carried out in the public interest, or for the performance of a task carried out in the exercise of official authority vested in the controller or in a third party to whom the PII is disclosed; or
- it is necessary for the legitimate interests pursued by the controller or by the third party to whom the PII is disclosed, and these interests are not overridden by the interests of the data subject.

11 Legitimate processing – types of PII

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

The DPA imposes more stringent rules for the processing of sensitive PII. The DPA distinguishes between sensitive and semi-sensitive personal data. Sensitive PII is data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership; and
- data concerning health or sex life.

The processing of sensitive personal data is generally prohibited unless one or more of the below conditions are met:

- the data subject has given his or her explicit consent;
- it is necessary to protect the vital interests of the data subject or of another person where the person concerned is physically or legally incapable of giving his or her consent;
- the processing relates to data that have been made public by the data subject; or
- it is necessary for the establishment, exercise or defence of legal claims.

Data concerning trade union membership may further be processed if necessary for the data controller's compliance with labour law obligations. Further exemptions apply, among others, to:

- the processing by a foundation or other non-profit-seeking body with a political; philosophical, religious or trade union aim of PII relating to the members of the body;
- certain processing by professionals within the public health care sector;
- processing required for the performance by a public authority of its tasks in the area of criminal law; and
- processing for the sole purpose of statistical or scientific studies of significant public importance.

Semi-sensitive personal data is data regarding:

- criminal offences;
- serious social problems (eg, long-term unemployment and information that a person qualifies for certain supplementary disability pensions); and
- other purely private matters (eg, results from personality tests, severe disciplinary measures in employment relationships, suicide attempts, family disputes, separation and divorce applications and adoption).

Semi-sensitive personal data may generally not be processed on behalf of a public authority, unless such processing is necessary for the performance of the tasks of the authority or if one of the grounds for processing sensitive data exists.

Private controllers may only process semi-sensitive personal data if one of the grounds for processing sensitive data exists or if necessary for the purpose of pursuing a legitimate interest and this interest clearly overrides the interests of the data subject.

Specific requirements apply to the processing of information on personal identification numbers (Central Office of Personal Registration (CPR) numbers).

Data handling responsibilities of owners of PII

12 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 controller must inform the data subject of:

- the identity of the data controller and his or her representative;
- the purpose of the processing for which the PII is collected;
- any further information that is necessary to enable the data subject to safeguard his or her interests, for example:
  - the categories of PII collected;
  - if providing PII is voluntary and consequences of not providing the requested data;

- the categories of recipients, if the information is to be disclosed; and
- the right to request access and correction.

When PII is collected from the data subject itself, notification must be provided at the time of collection. When PII is collected from other sources, notification must be provided as soon as possible and normally within 10 days. Where disclosure to a third party is envisaged notification must be provided no later than at the time of disclosure. There are no formal requirements in terms of the notification. Hence, the information may be provided orally, in writing or electronically, or printed on an application form, etc.

13 Exemption from notification

When is notice not required?

The obligation to notify does not apply if:

- the data subject is already familiar with the information;
- collection or disclosure is expressly required by law or regulations;
- the provision of notice proves impossible or would involve a disproportionate effort; and
- the data subject's interest in receiving notice is overridden by essential considerations of private interest, including the consideration for the data subject itself, or public interests, for example national or public security or defence, investigation and prosecution of criminal offences.

14 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 the data controller must inform the data subject whether PII relating to him or her is being processed.

At the request of the data subject, the data controller shall further rectify, erase or block data that turn out to be inaccurate or misleading or in any other way unlawfully processed. The data controller shall notify the third party to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the request of the data subject.

A data subject may at any time withdraw a prior consent to processing. Transfer of PII relating to a consumer for marketing purposes is generally subject to the data subject's consent. Disclosure and use of such data may, however, take place without consent if the processing relates to general data on customers that form the basis for classification into customer categories, unless overridden by the interest of the data subject and provided the data subject is given the opportunity to opt out prior to such transfer or use.

A data subject may object to automated decisions related to the data subject.

15 Data accuracy

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

The processing of data must be organised to ensure appropriate updating of the data. Furthermore, necessary checks must be made to ensure that no inaccurate or misleading data are processed. Data that turn out to be inaccurate or misleading must be erased or rectified without delay.

16 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 that is to be processed must be adequate, relevant and not excessive in relation to the purposes for which the PII is collected and the purposes for which they are subsequently processed. Whether or not the conditions are met should always be viewed in the context of the specific situation.

PII may not be kept for a longer period than necessary for the purposes for which the PII is collected. Continued retention must serve a legitimate purpose.

17 Finality principle

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

PII must only be collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes, in accordance with the finality principle.

18 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 any purpose that is incompatible with the purposes according to which the data were originally collected. Whether a new purpose is incompatible with the original purpose must be assessed on a case-by-case basis. Further processing that takes place exclusively for historical, statistical or scientific purposes is not considered incompatible with the original collection purposes.

Processing for a new compatible purpose may require a new notification to the data subject.

The data subject may consent to processing for new incompatible purposes.

Security

19 Security obligations

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

Data controllers are required to implement appropriate technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other unlawful processing. Hence, the data controller must ensure that the systems, organisation and workflows are designed in a way that the requirements in the DPA are fulfilled. The same applies to data processors.

The DPA does not offer more specific requirements to the method or level of security.

In the assessment of appropriate measures controllers are encouraged to perform a risk assessment considering the nature of PII and the possible harm to data subjects if PII should be unlawfully processed. The Agency has issued guidelines requesting encryption when sensitive PII and personal identification numbers are transferred via websites and is encouraging encryption and use of appropriate virus and malware protection, etc, for other communications. Furthermore, the Agency has issued various guidelines relating to IT security.

In relation to processing of PII by public authorities certain specific measures are required by the Executive Order on Security, including obligations to implement data processing policies and access restrictions, training and instruction of employees who process the PII, ensuring physical protection, logging access to data and securing digital communication, disposing of hardware and deleting data. If an external service provider (data processor) processes the personal data on behalf of the data controller, it will be the responsibility of the data controller to ensure that the relevant provisions in the order and the DPA are fulfilled through relevant binding agreements.

Although the order is only statutory for public authorities, private sector controllers are encouraged to be inspired by the order.

20 Notification of data breach

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

Currently there is no specific obligation to notify the Agency or affected individuals in case of a data breach. However, the Agency's interpretation of good practice compliance with the DPA requires the data controller to consider informing the Agency and affected individuals of serious breaches, based on a number of factors such as the number of individuals affected, the nature of the data and the potential harm to the data subjects. Not all breaches need to be reported. The Agency, if involved, may choose to publish the breach on its website and require the breaching data controller to take specific and appropriate action in respect of the breach.

Providers and owners of electronic communications and network services must notify the Danish Telecommunications Authority immediately if the provider or owner becomes aware of a security breach.

Internal controls

21 Data protection officer

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

There is currently no legal obligation to appoint a data protection officer under Danish law.

22 Record keeping

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

There are no explicit requirements for data controllers to maintain internal records or establish internal processes or documentation. The data controller must, however, be able to document its compliance with the DPA and other privacy regulation in the event the Agency undertakes inspections. Documentation may involve policies, processes and relevant permissions.

Registration and notification

23 Registration

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

The requirements are different for public authorities and private controllers.

Public authorities must notify the Agency of any processing if the processing includes sensitive or semi-sensitive data or data that otherwise are of a confidential nature. Exemptions exist for the processing of PII for certain specified purposes by public authorities.

Processing of PII by private sector controllers is generally subject to an obligation for the data controller to notify and obtain approval from the Agency to the processing. The DPA and related orders, however, include several exemptions upon which registration and notification are not required. Generally notification and approval are required for:

- processing that includes sensitive or semi-sensitive PII except:
  - where PII is not processed in a filing system (whether electronic or not) or not subject to other systematic processing;
  - processing of health data relating to employees in compliance with provisions laid down by law or regulations;
  - processing of employee data if it is necessary under collective or labour market agreements or for the purpose of withholding membership fees to employees' organisations;
  - processing by an association or similar body, to the extent that only data concerning the members of the association are processed,
  - processing carried out by public healthcare professionals (private hospitals are not included);
  - processing by lawyers and auditors of data related to clients;
  - processing of PII in connection with video surveillance;
  - processing of PII related to customers and other persons (excluding employees) by banks, insurance companies and other financial institutions in pursuance of a legal claim or as required complying with statutory obligations applicable to financial institutions;
  - testing of medicine and medical equipment and research projects in accordance with health sector legislation;
  - processing of PII by dating bureaus with the consent of the data subject; or
  - other specific exemptions provided by the DPA and related orders;
- processing of any PII carried out for the purpose of warning third parties against entering into business relations or an employment relationship with a data subject;
- processing of PII in a whistle-blower scheme;
- commercial disclosure of PII for assessment of financial standing and creditworthiness; and
- processing of any PII carried out for the purpose of professional assistance in connection with staff recruitment.

Data processors are not subject to the registration requirement.

24 Formalities

What are the formalities for registration?

Forms for notification and approval are available at the Agency's website (www.datatilsynet.dk). Forms may be completed and filed online. A fee of 2,000 kroner is payable. Notifications must include information on:

- the name, address and telephone number of the data controller and data processor, if any;
- the purposes of the processing;
- a general description of the processing;
- the categories of data subjects and the categories of PII processed;
- the recipients or categories of recipients to whom the PII may be disclosed;
- envisaged third-country transfers;
- general description of the security measures taken;
- date of commencement of the processing; and
- time for deleting the PII.

Once registered, the notification and approval are valid indefinitely and should not be renewed. Any changes to a filed notification must be notified to the Agency.

25 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 intended processing must not be initiated until the Agency has been notified and given its approval. Although the DPA provides for penalties for non-compliance this is rarely used.

26 Refusal of registration

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

Generally, the Agency does not refuse a notification for registration. If a notification is deemed incomplete or the intended processing is deemed unlawful, the Agency will advise and question on the specific matter in order to guide the data controller to become compliant. If the controller does not comply approval may be refused.

27 Public access

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

The register, including the completed notification form, is publicly available and may be accessed from the website of the Agency (www.datatilsynet.dk/fortegnelsen/om-fortegnelsen/). The register is only available in Danish.

28 Effect of registration

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

Not beyond fulfilling the statutory notification requirement.

Transfer and disclosure of PII

29 Transfer of PII

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

The data controller must ensure that its data processors implement the measures necessary for the data controller to comply with the DPA. The data controller must enter into a written agreement with the data processor stipulating that the data processor may only process PII in accordance with the data controller's instructions, that the data processor acts only on behalf of the data controller and that the data processor must implement technical and organisational security measures to prevent unlawful and unauthorised processing. The data controller must ensure it is able to effectively control that the data processor processes data in compliance with the agreement.

30 Restrictions on disclosure

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

Disclosure of PII to recipients other than a data processor may only take place to the extent such disclosure meets the legal grounds for processing of the specific category of data described in questions 10 and 11. Certain disclosures are subject to specific restrictions, for example:

- disclosure for the purpose of marketing requires the data subject's explicit consent;
- disclosure of PII to credit rating agencies;
- disclosure of identification numbers by private controllers may in the absence of consent only take place where such disclosure is a natural element of the ordinary course of a business and where the disclosure is required for an unambiguous identification of the data subject or if the disclosure is demanded by a public authority;
- public authorities' disclosure to credit information agencies of data on debts to public authorities is subject to specific regulation in the DPA; and
- disclosure of image and sound recordings containing personal data, which are recorded in connection with video surveillance for criminal prevention purposes, may only take place if the data subject has given his or her explicit consent, the disclosure is required by law, or the data are disclosed to the police for crime-solving purposes.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Transfers outside the European Economic Area are restricted, unless the country provides an adequate level of protection of the processing of PII. Whether a third country is deemed to have an adequate level of protection shall be assessed in the light of all circumstances related to the transfer, in particular the nature of the data, the purpose and duration of the processing operation, the law in force and security measures complied with in the country of destination.

The European Commission has published a list of third countries considered to provide for an adequate level of protection.

The US is generally not considered to offer adequate protection. However, a US company having signed up to the EU-US Privacy Shield is considered to provide adequate protection.

Transfer of data to a third country not deemed to have an adequate level of protection can however take place if:

- the data subject has given his or her explicit consent to a specific transfer;
- the transfer is necessary for the conclusion or performance of a contract with the data subject or concluded in the interest of the data subject between the controller and a third party;
- the transfer is necessary or statutory for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is made from a register that according to law is open to the public;
- the transfer is necessary in criminal proceedings; or
- the transfer is necessary to protect important public interests or to safeguard public or national security.

Finally, transfer of personal data to unsafe third countries may also take place if the transferor and transferee of PII have concluded EU model clauses for the export of personal data or if the transfer has been specifically approved by the Agency, or subject to Binding Corporate Rules approved by a Supervisory Authority.

32 Notification of cross-border transfer

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

The Agency's prior approval is generally required to transfer data to non-EEA countries if the transfer includes sensitive or semi-sensitive PII unless the transfer is based on the data subject's explicit consent or based on the EU standard model clauses without any changes (even the smallest change implies the Agency's permission). Exemptions from approval also exist in relation to transfers in the data subject's vital interest and transfers in criminal proceeding purposes and purposes of public and national security.

Please note that approval is required irrespective of whether the third country of destination is considered to have an adequate level of protection.

33 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 service providers and onwards transfers and even to transfers for use internally in an organisation.

Rights of individuals

34 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.

Subject to specific exemptions provided by the DPA, the data controller must upon request inform the data subject whether or not personal data relating to him or her are being processed. Where such data are being processed, the data subject must be informed of:

- the data being processed;
- the purpose of the processing;
- the categories of recipients of the data; and
- any available information as to the source of such data.

The data subject may direct the request to the data controller in writing or orally. The data subject may empower a third party to request access on the data subject's behalf. The request does not need to specify the exact processing activities to which the data subject is requesting access. Information must be provided within four weeks from receipt of the request, otherwise the controller must inform the person in question of the grounds and the time at which the decision can be expected to be available. If requested, the information must be provided in writing.

If the data subject requires written access, the data controller may require 10 kroner for every page; payment may, however, not exceed 200 kroner. Repeated requests may be rejected until six months after the last communication, unless the data subject can establish a specific interest.

The data subject's right to access is limited under the same conditions as exemptions to provide notice. See question 13. Further access to PII processed by courts and public authorities in criminal law matters is restricted.

Data that are processed on by public authorities in the course of their administrative procedures may be exempted from the right of access in accordance with the Act on Public Access to Documents in Administrative Files.

35 Other rights

Do individuals have other substantive rights?

Other rights of the data subject include the right to:

- object to the processing of data relating to him or her;
- object to disclosure of PII for marketing purposes;
- seek rectification, erasure or blocking of PII that turns out to be inaccurate, misleading or unlawful;
- withdraw consent;
- object to automated decisions related to the data subject; and
- file a complaint to the Agency.

36 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 must compensate for any damage caused by the unlawful processing of PII, unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of data.

Only actual damage is compensated.

37 Enforcement

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

An individual may file a complaint to the Agency in order to exercise his or her rights according to the DPA. Compensation may only be enforced by the courts.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

Any provision on the processing of PII in other legislation that gives the data subject better legal protection shall take precedence over the provisions in the DPA.

The DPA shall not apply to the extent such application violates the freedom of information and expression, as to which, see article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Supervision

39 Judicial review

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

No appeal to any other administrative authority against the decisions made by the Agency is available. Hence, the data controller may bring decisions made by the Agency to the courts.

Specific data processing

40 Internet use

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

The Danish Cookie Order implements the ePrivacy Directive's requirements for the use of cookies. Accordingly it is unlawful to store a cookie on a user's device, or gain access to such information, unless the user has consented thereto having been provided with comprehensive information about the storing of, or access to, the information.

Hence, the user should be guided to understand that by clicking through the website he or she accepts the use of cookies (cookies must not be placed or accessed before the user has given his or her consent). It is important that the information provided meets the specific requirements of cookie notice.

Even in the absence of consent, information may be stored, or accessed, if used only for the transmission of communications over electronic communications network, or necessary for the provision of an information society service explicitly requested by the end user.

In April 2013, the Danish Business Authority published new guidelines relating to the Danish Cookie Order. The guidelines provide useful information, including several practical examples as well as a technical guide to businesses and public authorities' approaches for the practical implementation of the provisions. There is also an English version of the guidelines.

41 Electronic communications marketing

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

A trader is not allowed to approach anyone by means of email, an automated calling system or fax for marketing purposes, unless the party concerned has requested the trader to do so (opt in requirement).

Where a trader has received a customer's electronic contact details in connection with a previous sale, the trader may market his or her own – similar – products or services to that customer by email, provided that the customer is given the option to decline commercial communications when providing his contact details and in any subsequent communication.

A trader must not send unsolicited marketing to a specific natural person using other means of remote communication if the person concerned has declined such communications from the trader or if the person has made an entry in the CPR that he or she has declined communications for such marketing purposes.

Marketing by telephone to consumers is generally prohibited in the absence of the consumer's specific request.

42 Cloud services

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

The DPA does not include regulation specifically governing the use of cloud computing services. Processing of PII in the cloud is subject to the same requirements as other processing of PII. The Agency has, however, in a number of decisions expressed the Agency's opinion on processing of PII in cloud computing services – in particular public authorities' processing of PII in cloud computing services.

Prior to the application of a cloud-based solution, the data controller must perform a risk assessment concerning all aspects of the planned use of the cloud solution to identify any security issues and the possibility of mitigating these issues. As for any use of a data processor, it is a requirement that a written contract is established according to which the processor shall act only on instructions from the controller and shall implement appropriate technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the DPA. Public authorities must further ensure that the data processor comply with the Executive Order on Security (see question 19).

The data controller must be able to ensure and control the data processor's compliance with the above.

The data controller must also ensure that PII are not transferred to unsafe third countries unless the necessary safety measures are put in place to provide for an adequate level of protection of PII (eg, EU model clauses). This implies, for example, that the data controller at any time must know the physical location of the serves providing the cloud, and have general access to audit that data processor's compliance with the safety requirements.

LUNDGRENS

Michael Gorm Madsen **mgm@lundgrens.dk**

Tuborg Havnevej 19
2900 Hellerup
Denmark

Tel: +45 3525 2535
Fax: +45 3525 2536
www.lundgrens.dk

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Primarily, data protection in Germany is governed by the Federal Data Protection Act (the Act). The Act is substantially based on the EU Data Privacy Directive 95/46/EC and is complemented by several individual state law regulations regarding data processing of public authorities. Furthermore, a number of smaller area-specific rules define separate treatment for the respective areas.

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 the illegal data processing. If the person does not provide the requested information to the DPA in time or does not duly cooperate in audit measures of the DPA, the DPA may issue a fine with an administrative financial penalty (€50,000).

3 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 two years. Such offences are only prosecuted if a formal complaint is filed by the public prosecution department of the responsible DPAs, the affected data subject or the responsible data owner itself. Besides criminal sanctions of the Act, owners 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 Act provides for a complex 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 €50,000; and
- serious breaches with an administrative financial penalty of up to €300,000.

Scope

4 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 Act is generally applicable to all federal public authorities, state public authorities and all non-public entities that are processing PII. However, the Act is subsidiary to various area-specific rules, which make a number of authorities or entities subject to special regulations.

5 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 Act 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 only covered partially by the Act. 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.

6 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 are the TKG and the German Code of Telemedia, which provide comprehensive area-specific rules on telecommunication and telemedia (internet) services.

7 PII formats

What forms of PII are covered by the law?

The Act 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 Act. According to the DPAs even email and IP addresses fall under PII.

8 Extraterritoriality

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

The Act generally applies the principle of territoriality, which limits the scope of the Act to its own jurisdiction and data owners or processors established in this jurisdiction. Under certain conditions the Act may also be applicable to data processing in the European Economic Area (EEA), if the data processor operates from Germany and does not have a place of business in the relevant EEA country. Likewise the Act can apply if a data processor within the EEA uses an establishment in Germany to collect and

process PII. If the data processor operates from outside the EEA and processes PII within the territory of Germany, the Act can also be applicable provided that the data processor uses equipment situated in Germany to collect or process PII.

9 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?

Basically all processing or use of PII is covered by the Act 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 19).

Legitimate processing of PII

10 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 to create, perform, or terminate a legal obligation or quasi-legal obligation with the data subject (eg, consumer agreement); or
- processing is necessary to safeguard the legitimate interests of the processor and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing or use (ie, the balance of interest test).

11 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 in order to protect vital interests of the data subject or of a third party, insofar as the data subject is unable to provide consent for physical or legal reasons;
- the data concerned has evidently been made public by the data subject;
- it is necessary in order to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in excluding such collection, processing or use; or
- it is necessary for the purposes of scientific research, where the scientific interest in carrying out the research project substantially outweighs the data subject's interest in excluding collection, processing and use and the purpose of the research cannot be achieved in any other way or would otherwise necessitate disproportionate effort.

Data handling responsibilities of owners of PII

12 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: the type of data; identification of the data controller; and the purposes of processing.

Additional information may be necessary, depending on the circumstances, in order to ensure lawful and proper processing (eg, the fact that personal information may be transferred outside the EU, possible third-party data disclosures, and individuals' data protection rights). 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 by the time of recording of the data or, if transferred to a third party, by the time of disclosure.

13 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:

- PII was recorded only because they may not be erased due to legal, statutory or contractual provisions on retention (commercial and fiscal law); or
- PII was acquired from generally accessible sources and notification would require a disproportionate effort due to the large number of cases concerned.

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.

14 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 Act does not provide the individuals any degree of choice or control over the use of their PII. This is not necessary because, in general, the consent of the individuals has to be obtained to process their data unless one of the legal permissions is applicable.

15 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.

16 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 owner lodges an objection with the controller and examination indicates that legitimate interests of the data owner due to his or her particular personal situation override the interest of the controller in such collection, processing or use; or in specific cases where PII are processed for advertising purposes or market or opinion research.

Instead of ceasing, the Act normally demands blocking PII in the event the individual disputes their accuracy and their accuracy or inaccuracy cannot be verified. Instead of being erased PII shall be blocked in the case that:

- they are processed for own purposes, as soon as knowledge of them is no longer needed to carry out the purpose for which they were recorded;
- erasure would violate retention periods set by law, statute or contract;
- there is reason to believe that erasure would be detrimental to legitimate interests of the data owner; or
- erasure would be impossible or would involve a disproportionate effort due to the special category of recording.

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 or market or opinion research. When summarised, PII are legitimately intended to be disclosed to third parties, or to be processed on behalf of third parties without consent of the individual for direct marketing or charity purposes, if the data controller takes adequate measures that the individual is informed 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.

17 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 they are processed.

PII must not be kept in a form that allows identification of the individual for longer than necessary for the purposes for which they were collected or subsequently processed.

PII should not be subsequently or further processed in a way that is incompatible with the purposes for which they were obtained (principle of finality).

Further, the Act 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 reduction and data economy). 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.

18 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 the 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 for the purposes of address trading or advertisement follow special rules for justification in the Act.

Security

19 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 at preventing unnecessary collection and further processing of PII.

The Act contains an annex that delineates the security measures to be taken, specifically these must include:

- preventing access by unauthorised parties to data processing facilities on which PII is processed and used (access control);
- preventing use by unauthorised parties of data processing systems (access control);
- taking care to ensure that those persons authorised to use a data processing system are only able to access PII within the scope of their access rights, and that personal data cannot be read, copied, modified or deleted without authorisation during processing, use and after recording (access control);
- taking care to ensure that, during electronic transfer or transportation or when being saved to data carriers, PII cannot be read, copied, modified or deleted without authorisation, and that it is possible to check and identify the points at which data transfer equipment is likely to be used to move data (transfer control);
- taking care to ensure that it will subsequently be possible to check and ascertain whether and by whom PII has been added to, modified in or deleted from data processing systems (data entry control);
- taking care to ensure that PII processed under the terms of the agreement can only be processed in accordance with the instructions issued by the controller (order control);
- taking care to ensure that PII is protected against sudden malfunctions or loss (availability control); and
- taking care to ensure that data collected for different purposes can be processed separately (separation control).

The data controller is furthermore required to execute an information security agreement (a written data processor agreement) with service providers (regardless 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 only select third-party service providers that offer adequate guarantees for technical and organisational information security.

20 Notification of data breach

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

Personal data breach notification is required if:

- one of the following data categories is concerned:
  - 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);
  - PII that is subject to professional or official secrecy;
  - PII concerning criminal acts or administrative offences;
  - PII on bank or credit card accounts;
- data has been transferred unlawfully or accessed otherwise by third parties; or
- this has or may have a serious impact on the rights or protected interests of the individual.

The data controller should notify the competent DPA and the individuals without delay. However, individuals should be informed as soon as appropriate measures to safeguard the data have been taken and notification would no longer endanger criminal prosecution. 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: advertisement of at least half a page in at least two daily national newspapers; or other means that would provide equivalent exposure in view of notifying the individuals.

Notification to the individuals concerned must include a description of the type of unlawful disclosure and recommendations for measures to limit possible negative consequences.

Notification to the DPA must include a description of the type of unlawful disclosure, recommendations for measures to limit possible negative consequences, possible consequences of the unlawful disclosure and a description of the measures undertaken by the controller as a result.

Internal controls

21 Data protection officer

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

The appointment of the data protection officer (DPO) is mandatory if the controller carries out automated processing with more than nine employees or regularly employs at least 20 employees in relation to non-automated processing. The appointment of a DPO also results in a notification exemption, so it is advisable to appoint a DPO to avoid notification obligations.

The DPA must be notified of the DPO's engagement. The DPO is autonomous and is responsible for supervising data controllers' compliance with the Act. The DPO will maintain a public register 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 until one year after the appointment terminates. 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.

Update and trends

On 14 April 2016 the European Parliament has finally adopted the long awaited EU General Data Protection Regulation (GDPR). The GDPR now becomes officially EU law and will directly apply in all EU countries, including Germany, replacing EU and national data protection legislation.

The GDPR will enter into force as from May 2018. By then national legislators are required to amend their local data protection laws in many aspects. It will be interesting to see how Germany reacts and which specific laws Germany will provide under the new GDPR set of rules. As companies are advised to prepare for the new rules as early as possible, this development should be observed with due care.

22 Record keeping

Are owners 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 34). 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 21), 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).

Registration and notification

23 Registration

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

The Act requires a general duty of notification prior to commencing data processing. Generally, notification is exempted if an internal DPO has been appointed; or the data processor processes the PII only for its own purposes, without employing more than nine employees and the individuals consent to the processing or the processing is necessary to conclude, perform or terminate a contract with the individual.

24 Formalities

What are the formalities for registration?

Registration can be consulted in the DPA's public register. The form for notifications to the DPA can be submitted in writing or via email or fax. There are no fees for notification.

Notifications are not subject to renewal. However, the data processor should inform the DPA of a change in the name or address of the data controller before such change becomes effective. Changes to information about processing must be notified prior to the implementation of the changes.

25 Penalties

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

Non-compliance with the registration requirement is subject to an administrative fine of up to €50,000. This also applies to registrations regarding any changes prior to the implementation or effectiveness of such changes.

26 Refusal of registration

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

There is no special obligation for the DPA to control the notifications prior to registration or to refuse an entry on the register. This is because the duty of notification lies with the data controller and no legal privileges are granted with entry to the register (see question 28).

27 Public access

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

The register is publicly available. No additional requirements have to be met to get access to it. Access, in particular, depends on the way the register is documented by the DPA, either automatically or manually. In most cases it is still documented manually.

28 Effect of registration

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

No legal effect is connected with entering the register of the DPA. The register only serves an information purpose: first to give the competent DPA some detail on the data processing and secondly to provide transparency for the affected individuals and the public, also for preparing claims against the data processor (eg, injunctive relief or even damages).

Transfer and disclosure of PII

29 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 Act. The conditions shown under question 19 apply to this kind of data processing. But this is only true for a processor being strictly bound to the instructions of the controller. 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 10 and 30.

30 Restrictions on disclosure

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

The term 'disclosure' is not defined in the Act, but relates to making PII public and transferring PII from the data controller to a third party other than a processor. Disclosure of personal data to another legal entity is only permitted if a legal ground is presented as mentioned in question 10; and such disclosure is not incompatible with the purposes for which the PII were initially collected.

As the Act does not include 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.

31 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 30.

Transfers of PII outside the EEA are only permitted if one of the exemptions listed in the Act 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 now 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.

32 Notification of cross-border transfer

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

A duty of notification applies only to the extent as outlined under question 23. 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 10 and 30).

33 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 29) or as an onward transfer. So 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

34 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 origin and recipients of the data) and, upon request, the purpose of the storage (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. 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 and free of charge. 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:

- 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);
- such is required to protect the overriding interests of the company (eg, if the continuity of the business would be jeopardised);
- 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, which is no longer needed for the original purposes, but retained due to the legal obligation.

35 Other rights

Do individuals have other substantive rights?

Individuals have the following rights:

- the right to be informed (notice requirement);
- the right to request to correct, supplement, delete or block PII relating to them that are inaccurate, incomplete or irrelevant for the purposes of the processing, or are being processed in any other way that infringes a legal provision;
- the right to object to processing of their PII if the processor bases the processing of PII on its proper legitimate interests (that 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 direct marketing; and
- the right to compensation if they suffer damage or distress as a result of a breach of the Act or other data protection provisions.

36 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 Act. This claim is not based on fault of the data owner if the data is processed automatically. For serious breaches the claim also covers injury to feelings; in all other cases actual damage is required.

37 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 Act 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

38 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 Act provides some distinctive provisions for data transfers to credit agencies, scoring, research institutions, media, storage of PII for purposes of privacy control and PII that are subject to any professional or official confidentiality.

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

Supervision

39 Judicial review

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

Fines of 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

40 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 e-Privacy 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. It is therefore advisable to at least meet the recommendations the EU article 29 group 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 EU Article 29 Working Party you will have to distinguish between various types of cookies in particular. However, in all cases, the website's privacy policy should contain a description of how the PII is processed. Additionally, the cookie user should grant the individual an opportunity to object against the use of its PII.

41 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 it wants to receive unsolicited marketing messages, has provided the email address where it 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.

42 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 19. Moreover, the DPAs have issued a guidance paper for using cloud computing services. According to this guidance paper the 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 31), 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/interoperability of the data, for example, in case of 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.

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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). 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. Telecom regulations, by and large, prevent the transfer of customer information 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 for 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 authority has powers.

3 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

4 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 the privacy rules have been notified as part of RSPP.

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.

5 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.

6 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.

RBI regulations on outsourcing also deal with the ability of banks to transfer data outside India. This is permitted, provided that: (i) the offshore regulator will not obstruct the arrangement or prevent inspections by the RBI or auditors; (ii) the availability of records to the management and RBI would withstand the liquidation of the offshore provider or the bank in India; (iii) the offshore regulator does not have access to the data simply because the data is being processed overseas; and (iv) 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.

7 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 on the basis of the format of the information, such as electronic as opposed to physical records.

8 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.

9 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?

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

10 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.

11 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

12 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 information, 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.

13 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 owner. It should also be noted that the privacy rules do not apply to the government.

14 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.

15 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.

16 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.

17 Finality principle

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

Yes. SPD 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 SPD 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.

18 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

19 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 prescribe 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.

20 Notification of data breach

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

No, it does not contain obligations to notify the regulator or individuals of breaches of security.

It may be noted that under banking regulations, the RBI has prescribed that banks must notify the RBI or Computer Emergency Response Team (CERT) or the Institute for Development & Research in Banking Technology for breaches of security.

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 webpages and websites. However, neither the IT Act nor any rules made thereunder require individuals or body corporates to mandatorily report cybersecurity incidents to CERT.

Internal controls

21 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 who will address discrepancies and grievances of providers of information. There is no requirement for appointment of a data protection officer.

22 Record keeping

Are owners 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.

Registration and notification

23 Registration

Are PII owners and/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.

Update and trends

There has been huge uproar over the right to privacy being a fundamental right guaranteed under the constitution of India. A case on this is currently pending before a constitutional bench of the Supreme Court of India. The decision of this case would lay down the privacy framework of the country.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 was passed by the Parliament in March 2016. The Act provides a legal backing to the Aadhaar number (ie, a unique identity number allotted to the citizens of India) and restricts the authorities from disclosing biometric information to any third party. However, the Act limits its application to privacy issues relating only to the use of the Aadhaar number and biometric information associated with Aadhaar. The Act is yet to be notified in the official gazette and is not in force yet.

There have been rumours for many years of a privacy bill being drafted by the government. The press information bureau recently reported that the government has initiated the process of drafting the legislation to protect the privacy of individuals breached through unlawful means, in consultation with various stakeholders. It is not known when the draft bill would be made available or be placed before the Parliament.

24 Formalities

What are the formalities for registration?

Not applicable.

25 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.

26 Refusal of registration

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

Not applicable.

27 Public access

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

Not applicable.

28 Effect of registration

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

Not applicable.

Transfer and disclosure of PII

29 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.

30 Restrictions on disclosure

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

There are no restrictions other than as stated above.

31 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.

32 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.

33 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

34 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.

35 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.

36 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.

37 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.

Exemptions, derogations and restrictions

38 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 19, 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

39 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

40 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.

41 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 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.

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

42 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 realting 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.

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The data protection regime in Ireland is 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 (e-Privacy Regulations) deal with specific data protection issues relating to use of electronic communication devices, and particularly with direct marketing restrictions.

The General Data Protection Directive (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 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;
- one-stop shop for 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.

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.

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 e-Privacy 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 the ODPC 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.

3 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 e-Privacy 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

4 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
- the personal data 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.

5 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 e-Privacy Regulations. The e-Privacy 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.

6 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, and has had an increasing focus on cybersecurity risks in recent years. 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 e-Privacy Regulations, which implement Directive 2002/58/EC (the e-Privacy Directive), and are of particular importance to providers of publicly available electronic communications networks and services, as well as businesses engaged in direct marketing.

7 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).

8 Extraterritoriality

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

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 are 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.

9 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?

Yes. 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.

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 increases the focus on processing activities, and data processors will have additional obligations once it comes into force.

Legitimate processing of PII

10 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 11) 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 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 12 and 15 to 19).

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.

11 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 10, 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

12 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.

13 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.

14 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.

15 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.

16 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.

17 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.

18 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 are 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.

Security

19 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.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and 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 e-Privacy 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.

Internal controls

21 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.

22 Record keeping

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

No. No such 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.

Registration and notification

23 Registration

Are PII owners and/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.

24 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.

25 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.

26 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.

27 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)).

28 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.

Transfer and disclosure of PII

29 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.

30 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 e-Privacy Regulations set out security measures for electronically stored data applicable to providers of publicly available electronic communications networks and services.

31 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 to is not on the approved lists above then transfer may nonetheless be possible in the following circumstances:

- where the ODPC authorises such (see following paragraph);
- 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.

Update and trends

The position in relation to cross-border transfers is under considerable scrutiny at present. In *Schrems*, delivered on 6 October 2015, the Court of Justice of the European Union (CJEU) declared the Safe Harbor regime invalid. Under Safe Harbor, personal data had been freely transferable from EU member states to US companies that had voluntarily signed up to Safe Harbor, despite an absence of federal US general data protection laws.

One of the main pillars of the CJEU decision in *Schrems* rested on the fact that, because certain US security and law enforcement agencies (such as the NSA) had broad access to the personal data of EU citizens transferred under Safe Harbor, without clear and precise limitations or appropriate safeguards on that access, US law failed to give adequate or 'essentially equivalent' protection to the data protection and privacy rights of EU citizens. On that basis, it was no longer permissible to justify transfers of personal data to the US on the basis of Safe Harbor.

The EU-US Privacy Shield (Privacy Shield) replaces the Safe Harbor framework and places stronger data protection obligations and standards on US companies. The Privacy Shield was formally adopted by the Commission on 12 July 2016, following its formal approval from all member states on 8 July 2016.

The Privacy Shield is only applicable to data transfers between the EU and US, and was designed to address the shortcomings in the Safe Harbor identified by the CJEU in *Schrems*. In that regard, the Privacy Shield differs from Safe Harbor in its inclusion of written commitments from the US, through the US Secretary of State and the Federal Trade Commission, to protect European data when it leaves the EU and enters the US, including protection against indiscriminate mass surveillance and specific preconditions for access to such data. It also provides for a number of redress mechanisms for EU citizens.

It should be noted that the Privacy Shield is not immune to challenge or modification, based on the CJEU's rationale in *Schrems*. Furthermore, with the recent request from the Irish Data Protection Commissioner to the Irish High Court, directly as a result of the decision in *Schrems*, that a case be stated to the CJEU concerning data transfers to the US based on the concerns with regard to the validity of use of the SCCs are also being crystallised. The case before the High Court is due to be heard in spring 2017.

Significant changes to the data protection regime applicable in Ireland will be effected from 25 May 2018, when the GDPR comes into effect. A number of the more significant changes are summarised throughout this chapter.

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 BCR are submitted to the ODPC for approval. The EU standard contractual clauses (SCC) 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 SCC does not require approval of the ODPC. The ODPC also has the power to approve contractual clauses that do not necessarily conform to the SCC, but in practice is only likely do so where there is a strong justification for not using the SCC.

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 (see further on this in Update and trends).

32 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.

33 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

34 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.

35 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 12 and 15 to 19) will all be impacted by these changes.

36 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.

37 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. However, certain actions by data processors or controllers can attract either civil or criminal liability.

Exemptions, derogations and restrictions

38 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

39 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).

Specific data processing

40 Internet use

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

Under the e-Privacy 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.

41 Electronic communications marketing

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

Under the e-Privacy 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.

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

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.

42 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.

Japan

Akemi Suzuki
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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The Act on the Protection of Personal Information of 2003 (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.

A limited portion of the Amendment came into effect on 1 January 2016 while the remainder, which would have a major impact on private businesses, remains unenforced. The date of full enforcement has not been published, but it will be no later than 9 September 2017.

At the time of writing, the APPI is implemented by a number of industry- or sector-specific administrative guidelines compiled by governmental ministries. As of November 2015, as many as 38 administrative guidelines covering 27 sectors exist. 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 Personal Information Protection Committee (the Committee) was established on 1 January 2016 as a cross-sectoral, independent governmental body to oversee the APPI. Until the full implementation of the Amendment, different governmental ministries enforce the APPI in the respective sectors and industries that they supervise. Governmental ministries have the following powers under the APPI:

- to require reports from PII data users (as defined in question 9) for their businesses over which the respective ministries have jurisdiction;
- to give advice necessary for the handling of PII to PII data users;
- upon violation of certain obligations of any PII data 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.

Following the full introduction of the Amendment, the Committee will generally take over the foregoing powers and additionally will be given the power to conduct an on-site inspection of the offices or other premises of PII data users.

3 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 person:

- fails to comply with any order issued by the competent governmental ministry, or the Committee following the full implementation of the Amendment (subject to penal servitude of six months or less or criminal fine of ¥300,000 or less); or
- fails to submit reports, or submits untrue reports, as required by the competent governmental ministry, or the Committee following the full implementation of the Amendment (subject to criminal fine of ¥300,000 or less).

The Amendment will also introduce additional criminal penalties under the following circumstances:

- a person refuses or interrupts an on-site inspection of the offices or other premises by the Committee (subject to a criminal fine of ¥300,000 or less); 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 one year or less or a criminal fine of ¥500,000 or less).

If the foregoing offences are committed by an officer or employee of a PII data user that is a judicial entity, then the entity itself may also be held liable for a criminal fine.

Scope

4 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.
- Private businesses that have owned PII of less than 5,000 individuals in their electronic or manual database at any time in the past six

months are also exempt (small business exception). This exception, however, will be abolished under the Amendment.
- 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.

5 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.

6 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.

7 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 comprising a PII database is called PII data.

The Amendment will broaden the definition of PII by expressly including 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.

In addition, the Amendment will introduce 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 will not be considered PII.

8 Extraterritoriality

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

Currently, it is widely considered that the APPI does not have extraterritorial application. 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.

However, following the full implementation of the Amendment, the APPI will apply when PII owners use or process, outside of Japan, such PII of individuals residing in Japan as was obtained in connection with the provision of goods or services by the PII owners.

9 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?

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 10);
- to notify the relevant individual of, or publicise, the purposes of use prior to or at the time of collecting PII (see question 12);
- to not use deceptive or wrongful means in collecting PII (see question 10);
- to endeavour to keep its PII data accurate and up to date to the extent necessary for the purposes of use (see question 15);
- to undertake necessary and appropriate measures to safeguard the PII data it holds (see question 19);
- to conduct necessary and appropriate supervision over its employees and its service providers who process its PII data (see question 19); and
- not disclosing the PII data to any third party without the consent of the individual (subject to certain exemptions) (see question 29).

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 12);
- to provide, without delay, a copy of retained PII data to the relevant individual upon his or her request (see question 34);
- 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 14);
- 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 14); 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 14).

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

10 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.

11 Legitimate processing – types of PII

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

Presently, the APPI does not have special rules for specific types of personal data. Some of the administrative guidelines for the APPI adopted by governmental ministries, however, impose stringent restrictions on the collection, use and disclosure to third parties of certain sensitive data.

The Amendment will introduce the concept of 'sensitive personal information,' which includes race, beliefs, social status, health and criminal records. Collection or disclosure under the 'opt-out' mechanism of sensitive personal information without the consent of the relevant individual will be generally prohibited.

Data handling responsibilities of owners of PII

12 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 PPI 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 30). Such information includes types of information being disclosed and 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: name of the PII data owner; all purposes for which retained PII data held by the PII data owner is used generally; 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.

13 Exemption from notification

When is notice not required?

There is an exception to the first notice requirement mentioned in question 12 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 acquisition of the relevant PII data.

14 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 34);
- 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.

15 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. In addition, the Amendment requires that all PII data users endeavour to erase, without delay, such PII data that is no longer needed to be used.

16 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 Amendment, PII data users must endeavour to erase, without delay, such PII data that is no longer needed to be used.

17 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 12. 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 an individual and it is difficult to obtain consent of the affected individual.

18 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?

Purpose for use may be amended, without the consent of the relevant individual, to the limited extent that would be reasonably deemed to be reasonably related to the previous purposes. PII may be used for such amended purposes, provided that the amended purposes are notified or made available to the affected individuals.

Under the Amendment, purpose for use may be amended to the extent reasonably deemed to be related (as opposed to 'reasonably' related) to the previous purposes. The implications of this change are unclear at this point.

Security

19 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 in many of the administrative guidelines for the APPI. For instance, the administrative guidelines prepared by the Ministry of Economy, Trade and Industry (METI Guidelines) set forth a long list of four types of mandatory or recommended security measures – organisational, personnel, physical and technical measures.

20 Notification of data breach

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

The APPI, either before or after the Amendment, 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 regulator or an accredited personal information protection organisation, if applicable, is generally required or recommended under most administrative guidelines for the APPI. In addition, such guidelines generally recommend or require notification to the affected individuals or public announcement in case of serious security breach incidents.

Thresholds for or exceptions to such requirement or recommendation vary depending on individual guidelines – the METI Guidelines, for instance, recommend reporting to the METI, as opposed to an accredited personal information protection organisation, if sensitive information or credit card information was possibly compromised. On the other hand, under the METI Guidelines, neither notification to the affected individuals nor public announcement is necessary if the lost or disclosed data was protected by advanced encryption or other security enhancing measures and the risk of violation of privacy or other rights of the relevant individuals are nil or very low.

Internal controls

21 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 METI Guidelines and a number of other administrative guidelines on the APPI. The METI Guidelines do not provide for qualifications, roles or responsibilities of a chief privacy officer.

22 Record keeping

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

PII data users are generally required under applicable administrative guidelines on the APPI to establish internal processes to safeguard the PII data.

Under the Amendment, 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 verify how the PII data was acquired by such third parties and keep records of such verification.

Registration and notification

23 Registration

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

Currently, there is no such registration requirement in Japan. Under the Amendment, PII data users who disclose PII data (other than sensitive personal information) under the 'opt-out' mechanism are required to submit a notification of such disclosure to the Committee.

24 Formalities

What are the formalities for registration?

Formalities for registration are not applicable. Formalities for a notification of disclosure under the 'opt-out' mechanism mentioned in question 23 are yet to be published by the government. Upon the receipt of such notification, the Committee will publicise certain information included in the notification.

25 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.

26 Refusal of registration

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

Not applicable.

27 Public access

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

Not applicable.

28 Effect of registration

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

Not applicable.

Transfer and disclosure of PII

29 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.

30 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:

- 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; and certain information regarding such disclosure is notified, or made easily accessible, to the individual prior to such disclosure;
- 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.

With respect to disclosure under the opt-out mechanism mentioned above, the Amendment requires that it must also be notified in advance to the Committee.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

At present, there are no general restrictions on the ability of a data owner to transfer PII outside Japan. Under the Amendment, however, transfer of PII data to a third party located outside of Japan will be subject to prior consent of the relevant individual except to the extent that the third party is located in foreign countries that the Committee determines warrant the equivalent level of protection of PII as Japan, or that the relevant third party has established on a continuous basis the equivalent level of protective measures as PII data users are required to establish under the amended APPI. At the time of writing, the Committee has not published its decision on the countries or businesses that meet the respective equivalency test. It is generally anticipated that transfer of PII data to foreign businesses certified under the APEC Cross-Border Privacy Rules will not be subject to the requirement to obtain prior consent of the individuals.

32 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.

33 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 31 under the Amendment will be applicable to transfers to service providers. They may also be applicable to onward transfers as long as the transferors of such onward transfers are subject to the APPI as amended.

Rights of individuals

34 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.

Currently, 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.

35 Other rights

Do individuals have other substantive rights?

In addition to the obligations set forth in question 14, 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.

36 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.

37 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 36) is enforced through the judicial system. With regard to violations by PII data owners of the obligations described in questions 34 and 35, currently, individuals do not have any statutory right to demand enforcement by the competent governmental ministry. The ministry may, however, recommend PII data owners to undertake measures necessary to remedy such violations if it deems it necessary to do so for protection of individuals' rights.

Under the Amendment, individuals may exercise their rights described in questions 34 and 35 through the judicial system, provided that they first request the relevant PII data owners to perform such obligations and two weeks have passed after such request was made.

Exemptions, derogations and restrictions

38 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

39 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 relevant supervising ministry or the Commission takes administrative actions against a PII data user, the PII data user will generally be able to challenge the actions judicially.

NAGASHIMA OHNO & TSUNEMATSU

Akemi Suzuki **akemi_suzuki@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

Specific data processing

40 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.

41 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.

42 Cloud services

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

The precursor of the Committee published regulatory guidance with respect to the use of cloud server services to store personal information obtained through the use of stored individual social security and tax numbers (specified personal information). Based on the guidance, the use of cloud server services to store specified personal information constitutes disclosure to outsourced processing service providers unless it is ensured by contract or otherwise that the service providers are properly restricted from accessing specified personal information stored on their servers. If the Committee is to take the same stance with respect to the storage of PII on third-party cloud servers, 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 29). Additionally, under the Amendment PII data users would need to confirm that the service providers offer functions of record-keeping (see question 22) and also 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 31).

Luxembourg

Marielle Stevenot, Rima Guillen and Charles-Henri Laevens

MNKS

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Directive 95/46/EC on data protection has been implemented in Luxembourg through the Law of 2 August 2002 relating to the protection of individuals in relation to the processing of personal data as last modified by the Laws of 27 July 2007 and 28 July 2011 (the Data Protection Law). The Law aims to protect the freedom and fundamental rights of individuals, notably their private life, in relation to the processing of their personal data.

The Law of 30 May 2005 for the protection of individuals in relation to the processing of personal data in the electronic communications sector as last modified by the Law of 28 July 2011 (the Electronic Communication Law) aims at implementing Directive 2009/136/EC on consumer protection and users' rights in relation to the processing of personal data and the protection of privacy in electronic communications.

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 (the National Commission) is responsible for enforcing data protection rules. It deals with requests and complaints made by data subjects. It must also further investigate any complaint and can temporarily suspend data processing. It has the power to order the deletion or the destruction of data, or prohibit further processing and report the case to the public prosecutor. Data subjects are kept informed of the progress of their complaint.

To perform its responsibilities, the National Commission has the power to investigate and collect all the necessary information. Notably, it can:

- access any data being processed, to carry out all necessary investigations;
- access premises where data processing takes place;
- block, delete or destroy data being processed, or temporarily or definitively prohibit such processing;
- order partial or total publication of the prohibition in newspapers or other means, at the expense of the sanctioned person; and
- engage in legal proceedings to enforce the Data Protection Law.

3 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 Data Protection Law provides for criminal sanctions that range from imprisonment of between eight days and one year and a fine of between €251 and €125,000, or only one of these penalties in case of breach of the Data Protection Law.

The National Commission has the statutory power to investigate and bring legal actions and may be approached by any person with a request relating to respect of his or her fundamental rights and freedoms as regards any data processing. The National Commission's position is not binding upon the public prosecutor.

If confronted with processing that is contrary to the provisions of the Data Protection Law, the National Commission may block, delete or destroy data being processed or prohibit such processing. Moreover, the National Commission may order the partial or integral publication of the prohibition by any means at the expense of the sanctioned person.

In order to claim for damages, individuals must bring a civil action before an examining magistrate.

Scope

4 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?

Processing carried out by an individual exclusively for personal or domestic activities is not covered by the Data Protection Law.

Data processing for criminal investigations and judicial proceedings are subject to specific rules, for instance, the Criminal Investigation Code and the Civil Procedure Code.

Additionally, certain exemptions apply, if necessary, in order to balance the right to privacy with freedom of speech, relating to data processing exclusively with journalistic, artistic or literary purposes.

5 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 Law of 11 August 1982 concerning the Protection of Privacy, the Electronic Communication Law and a Grand-Ducal Regulation of 24 July 2010.

Unsolicited electronic commercial communications are regulated by two different Laws:

- the Electronic Communication Law of 30 May 2005 for the protection of individuals in relation to the processing of personal data in the electronic communications sector, dealing with the sending of communications by a provider of electronic communication services; and
- the Law of 14 August 2000 on electronic commerce, dealing with the sending of communications by a provider of information society services.

The processing in relation to surveillance and surveillance at the workplace is governed by articles 10 and 11 of the Data Protection Law.

6 Other laws

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

A Grand-Ducal Regulation of 2 October 1992 relates specifically to the terms and conditions of use of personal data in medical databases, their use for therapeutic purposes, for research and disclosure to third parties.

Under the Law of 29 March 2013 on the organisation of the criminal record and the exchange of information extracted from criminal records

between member states of the European Union, the employer can, in the framework of the staff management and hiring process, request from the concerned person that they produce an extract of his or her criminal record (Bulletin No. 2). Bulletin No. 2 includes any and all convictions of the same person, except the convictions to imprisonment with a suspension period of less than six months, with or without a probationary period. It is important to note that the employer can process the data related to the criminal record only for the purpose of human resources management.

The criminal record extract provided to the employer in compliance with the Law of 29 March 2013 and the data contained therein cannot be stored, even as a copy, for more than 24 months from the date mentioned on the criminal record extract.

Other specific laws or grand ducal regulations apply to specific sectors such as rail, police or tourist accommodation.

7 PII formats

What forms of PII are covered by the law?

The Data Protection Law defines 'personal data' as any information of any type regardless of the type of medium, including sound and image, relating to an identified or identifiable natural person (data subject). Natural persons will be considered to be identifiable if they can be identified directly or indirectly, in particular by reference to an identification number or one or more factors specific to their physical, physiological, genetic, mental, cultural, social or economic identity.

8 Extraterritoriality

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

The Data Protection Law applies to any data processing implemented by a PII owner:

- established in Luxembourg; or
- not established in Luxembourg or in another EU country, but having recourse to processing means that are located in Luxembourg (except for processing means used for transit purposes only).

9 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?

The Data Protection Law defines the 'processing of personal data' as any operation or set of operations performed upon personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

The Data Protection Law distinguishes between the 'data controller', who determines the purposes and means of processing personal data, and the 'data processor', who processes personal data on behalf of the PII owner. It should be noted that the purposes and methods of processing personal data may be determined jointly by co-controllers.

The Data Protection Law does not distinguish between the data controller or processor and the data owner.

Legitimate processing of PII

10 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?

In addition to consent, which is not systematically necessary nor sufficient, the Data Protection Law provides that data processing is legitimate if:

- it complies with a legal obligation to which the PII owner is subject;
- it fulfils a task in the public interest, or in exercising official authority vested in the PII owner or in a third party to whom the data is disclosed;
- it takes place in performance of a contract to which the data subject is party, or in taking steps at the request of the data subject before entering into a contract;
- the purposes of the legitimate interests pursued by the PII owner, or by the third party or parties to whom the data is disclosed, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject; or
- it protects the data subject's vital interests.

Processing for surveillance reasons at the workplace cannot be carried out by the employer if the employer is the controller, except in the following cases (article L261-1, Employment Code):

- for the safety and health of employees;
- for the protection of the company's goods;
- for the control of the production process (provided this control only applies to the machines);
- for the occasional monitoring of the production process, or of the performance of employees, provided this measure is used to determine exact salaries; or
- in the framework of a flexitime working organisation.

Also, some specific types of data require specific cases of legitimacy (eg, sensitive data).

11 Legitimate processing – types of PII

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

Specific rules apply to the processing of sensitive data, which is, in principle, prohibited.

Sensitive data is defined as data relating to:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership; and
- health or sexual preference, including genetic data.

However, in limited circumstances processing this data is permitted if the conditions listed by the Data Protection Law are fulfilled. Express consent of the data subject is one of these circumstances. Other circumstances include:

- processing necessary to comply with the PII owner's employment law obligations and specific rights;
- processing necessary to protect the vital interest of the data subject where consent cannot be physically or legally given;
- the data subject has obviously made the data public;
- processing carried out by certain non-profit organisations; and
- processing necessary for establishing or defending legal rights.

Certain other types of specific data processing such as those regarding credit solvency, surveillance and surveillance at the workplace, and biometric data are subject to prior authorisation from the National Commission.

Data handling responsibilities of owners of PII

12 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?

When the data is collected directly from the data subject, the PII owner must provide the data subject at least with the following information:

- the identification of the PII owner and of his or her representative, if any;
- the purpose of the processing for which the data is intended; or
- any further information such as the categories of recipients to whom the data might be disclosed, whether answering the questions is compulsory or voluntary, as well as the possible consequences of failure to answer, the existence of the right of access to data concerning the data subject and the right to rectify them.

In addition, when the data is not collected directly from the data subject, the PII owner must inform the data subject of the categories of data concerned by the processing.

As regards timing, when data is collected directly from individuals, such individuals shall be informed of the processing at the time the data is collected. When data is collected indirectly from individuals, such individuals shall be informed of the processing at the time the data is transferred to third parties.

13 Exemption from notification

When is notice not required?

The obligation to inform individuals is subject to derogations notably when the processing is necessary to safeguard national security, defence or public safety. Other exceptions occur as regards the prevention, recording and prosecution of criminal offences or in case of an important economic or financial interest of the state or the European Union.

14 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 mentioned in question 12, there is an information requirement regarding data subjects.

In addition, data subjects have the right to:

- access information relating to them, free of charge, at reasonable intervals and without excessive waiting periods;
- request that the PII owner rectify or delete data, especially when such data is incomplete or inexact;
- request from the PII owner details about the personal information on record and its use; and
- object, free of charge, to the processing of their data, for legitimate reasons relating to their specific situation.

15 Data accuracy

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

The Data Protection Law requires the PII owner to ensure that the latter processes the data in a 'fair and lawful manner'. Therefore, the data shall be:

- collected for specified, explicit and legitimate purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed; and
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure information that is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified.

16 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 restriction concerning the amount of data collected, but the general principle is that it should not be excessive in view of purposes.

It should be noted that a disposition of the Data Protection Law requires that any interconnection of data that is not expressly provided by law or regulation must be authorised by the National Commission. The Law also sets out the conditions that the interconnection must meet.

No specific rules are provided by the Data Protection Law concerning the particular duration of the conservation of data, but it gives a general principle: the data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed.

In addition, the National Commission has set out certain guidelines through its practice for the duration of the conservation of specific kinds of data (eg, data collected for the purpose of surveillance at the workplace may not be kept more than six months).

In general, the National Commission analyses whether the retention period is not excessive on a case-by-case basis.

17 Finality principle

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

The data is collected for specified, explicit and legitimate purposes and shall not be processed in a way that is incompatible with those purposes.

18 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?

A single exception is enshrined by the Data Protection Law in the case of a subsequent processing of data for historical, statistical or scientific purposes. Otherwise, the use of PII for new purposes is prohibited unless the data subjects have given their prior consent.

Security

19 Security obligations

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

PII owners must take all appropriate technical and organisational measures to ensure protection of the data they process against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, in particular where the processing involves transmitting data over a network, and against any other unlawful processing.

In practice, a PII owner must set up different security measures, depending on the risk of privacy breach, the state of the art and costs relating to the implementation of these measures.

Generally, these measures consist of:

- preventing physical and logical unauthorised access to the data and access to, or use of, the information system where the data are stored;
- safeguarding data by creating backups;
- preventing data from being read, copied, amended or deleted in the event of disclosure or transport of such data; and
- monitoring of transmissions, transport and availability of the data.

In case of outsourcing of data, refer to question 29.

20 Notification of data breach

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

Under the Data Protection Law, there is no requirement to notify personal data security breaches to data subjects or the national regulator; however, a description of measures, and of any subsequent major change to these measures, must be communicated to the National Commission within 15 days upon request.

The Electronic Communication Law of 2005 provides that in a case of violation of personal data, the provider of electronic communication services must promptly inform the National Commission of such violation.

When the violation of personal data is likely to adversely affect the personal data or privacy of a subscriber or an individual, the provider must also notify the subscriber or individual concerned of such violation without unnecessary delay.

The notification to the data subject is, however, not required if the provider can prove to the National Commission that he or she has implemented appropriate technological protective measures to the data concerned by the security breach.

Internal controls

21 Data protection officer

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

The PII owner may designate a privacy official (also called data protection officer), but it is not mandatory.

Such appointment releases the PII owner from the obligation to notify most of the data processing to the National Commission (except for the processing of data for surveillance and surveillance at the workplace purposes) as the data protection officer will be in charge of ensuring compliance with the Data Protection Law and liaising with the National Commission.

To accomplish their missions, data protection officers have a right of investigation and of information. Although they may be employees of the PII owner, they must be independent for the performance of their task and be allocated sufficient time to do so.

Data protection officers must notably:
- ensure proper application of the applicable laws and regulations on data protection; and
- submit to the National Commission a register containing a list of the data processing they monitor in the name of a PII owner.

22 Record keeping

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

The Data Protection Law does not specifically provide for any obligation to maintain internal records as regards data processing.

Registration and notification

23 Registration

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

Depending on the type of data to be processed and the purposes of the processing, the PII owner may have to comply with some prior administrative formalities before starting the data processing.

A number of types of processing are exempted from any prior notification requirement, under certain conditions, specific to each exemption. There are 19 exemptions (including, for example, processing for the following purposes: management of the salaries of persons working for the PII owner, of job applications and recruitment and of the personnel of the data processor, accountancy and management of clients and providers). It must, however, be noted that some of the exemptions and conditions attached thereto are not straightforward and thus need interpretation.

24 Formalities

What are the formalities for registration?

Such formalities consist of prior notification to, or prior authorisation from, the National Commission. The principle is that any data processing is subject to prior notification except where prior authorisation is required by the National Commission or when the data processing is exempted by the law.

Processing submitted to prior authorisation from the National Commission includes, for example, processing of genetic data, processing relating to the credit status and solvency of the data subjects (when carried out by persons not acting in financial sector), data processing operations for historical, statistical or scientific purposes, or data processing operations for surveillance and surveillance at the workplace. Prior authorisation only concerns processing operations that are likely to present specific risks to the rights and freedoms of data subjects.

The notification form will include at least the following information:
- the name and address of the PII owner and of his or her representative, if any;
- the background to the legitimacy of the processing;
- the purpose or purposes of the processing;
- a description of the category or categories of data subjects and of the data or categories of data relating to them;
- the recipients or categories of recipients to whom the data might be disclosed;
- the third countries to which it is proposed to transfer the data; and
- a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing.

No renewal is needed if no modification has been made to the processing of data. If the processing is stopped, it shall be communicated to the National Commission.

The cost for a notification is in principle €125. The notification of a change in an existing processing amounts to €75. These amounts are reduced by €25 in case an additional notification is made by electronic means.

The same amounts are applicable for a prior authorisation.

25 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 a unique set of sanctions that also apply to failure to notify or ask for prior authorisation. The criminal sanctions may be imprisonment of between eight days and one year and a fine ranging between €251 and €125,000, or only one of these penalties. In addition, the CNPD may take administrative disciplinary sanctions and the data subject can bring an action for damages before the courts.

26 Refusal of registration

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

The National Commission may refuse the application in only two situations:
- the notification is not complete or does not comply in any way with formal grounds (the National Commission does not do a substantive examination of the notifications); or
- the request for prior authorisation does not comply with the criteria for lawful processing (in case of an application for a prior authorisation, the National Commission does a substantive examination).

27 Public access

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

The National Commission holds a public register of processing operations, accessible on its website in French or in German (www.cnpd.public.lu/fr/registre/application/index.html), which displays processing operations notified to or authorised by the National Commission.

28 Effect of registration

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

The PII owner must not start processing data before notifying the National Commission (in principle, the data controller should wait for the receipt of acknowledgment) or before obtaining the authorisation of the National Commission, depending on the nature of the processing.

Transfer and disclosure of PII

29 Transfer of PII

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

The Data Protection Law covers the outsourcing of data.

If the processing is carried out on behalf of the PII owner, the latter must choose a processor that provides sufficient guarantees regarding the technical and organisational security measures pertaining to the processing to be carried out. It is up to the PII owner as well as the processor to ensure that said measures are respected.

Any processing carried out on another's behalf must be governed by a written contract binding the data processor and providing in particular that the processor will act only on instructions from the PII owner.

30 Restrictions on disclosure

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

Disclosure is subject to general data processing principles. Data subjects have to be informed of the transfer.

Transfers of data outside the EEA may take place only where the country in question provides an adequate level of protection according to the European Commission and complies with the provisions of the Data Protection Law.

In case of data processing for the purpose of surveillance, the data transfer to third parties may occur only upon consent of the data subject.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Transfer of data within the EEA

To the extent data subjects have been properly informed of the transfer, data can be freely transferred within the EEA.

Update and trends

After four years of political discussion, the General Data Protection Regulation (GDPR) was finally adopted by the European Parliament on 14 April 2016. The GDPR will replace Directive 95/46/EC. A transitional period of two years is provided until the GDPR becomes fully enforceable in the member states.

The GDPR shall be directly applicable in all member states without the need for implementing national legislation.

The GDPR shall pursue the objective of ensuring a consistent and high level of protection of natural persons, and addresses the following fundamental issues:

- reinforcing individuals' rights;
- strengthening the EU internal market;
- ensuring stronger enforcement of the rules;
- streamlining international transfers of personal data; and
- setting global data protection standards.

Transfer of data outside the EEA

In principle, data cannot be transferred outside the EEA, except if the destination country ensures an adequate level of protection for the rights and freedoms of individuals. The European Commission has recognised several countries outside the EEA ensuring an adequate level of protection, a list of which is on its website (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).

A transfer to a country that does not offer an adequate level of protection can still, however, be possible provided:

- the data subject has given his or her consent;
- it is necessary to perform a contract to which the data subject and the PII owner are parties, or to enter into this agreement at the data subject's demand;
- it is necessary for the performance or the conclusion of a contract to which the PII owner or the data subject are parties;
- it is necessary or legally mandatory for reasons of substantial public interest or for establishing, exercising or defending legal rights;
- it is necessary to protect the vital interest of the individual; or
- it comes from a public register.

In addition, transfers outside the EU can be authorised where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. Such adequate safeguards may result from appropriate contractual clauses (standard data protection clauses) or binding corporate rules, according to the Article 29 Working Party.

Contractual clauses and binding corporate rules

The data exporter and the data importer may execute standard contractual clauses approved by the European Commission (also known as the model clauses). The Commission has so far issued two sets of standard contractual clauses for transfers from data controllers to data controllers established outside the EU/EEA (Decision 2001/497/EC: Set I; Decision 2004/915/EC: Set II) and one set for the transfer to processors established outside the EU and EEA (Decision 2010/87/EU (and repealing Decision 2002/16/EC)).

Multinational organisations can use binding corporate rules (BCR) to transfer personal data within the group. This is an alternative to the company having to sign standard contractual clauses each time it needs to transfer data to a member of its group and may be preferable where it becomes too burdensome to sign contractual clauses for each transfer made within a group. It should be noted that the BCR do not provide a basis for transfers made outside the group.

Transfer to the United States

The US is not a country considered to be offering an adequate level of protection of data. Thus, any transfer of personal data is subject to restrictions outlined above. Until October 2015, in order to ease the relationships between the United States and the EU, an US-EU Safe Harbor framework allowed any transfer of personal data to a business or organisation in the US provided the recipients adhered to the 'safe harbour' principles (Safe Harbor). The Safe Harbor arrangement consisted of data protection principles to which American undertakings could subscribe voluntarily. Therefore, it was based on the self-assessment and self-certification of private companies.

On 6 October 2015, the Court of Justice of the European Union issued a ruling in the case *Schrems v Data Protection Commissioner* (Case C-362/14), declaring as invalid the European Commission's Decision 2000/520/EC of 26 July 2000, which formed the basis of data transfers between the EU and the US.

As a consequence, companies now have to use alternative grounds to transfer data to the US in accordance with the requirements of both the Data Protection Act and the EU Data Protection Directive 95/46/EC.

An alternative solution has been negotiated between the US and the EU. On 12 July 2016, the European Commission approved the EU-US Privacy Shield. This political agreement aims to protect the personal data of EU member state nationals transferred to the US. The new EU-US Privacy Shield framework ensures an adequate level of protection of personal data transferred to the US and gives clear safeguards as to the possibility for the US government to access data. Once US companies have had an opportunity to review the framework and update their compliance, they will be able to certify with the Department of Commerce.

32 Notification of cross-border transfer

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

Authorisation from the National Commission is required to transfer data outside the EEA, only when the circumstances listed in question 31 do not apply.

33 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 answer to this question is not clearly provided by the Data Protection Law, but, taking into consideration the spirit of the law, it can be said that PII owners must ensure that onward transfers may only be undertaken in circumstances where at least the same level of privacy protection as is required under the Data Protection Law is provided.

Such a result may only be obtained provided the onward transfer is made to a country providing an adequate level of protection, under contractual clauses, or to a processor adhering to Safe Harbor principles, etc.

Rights of individuals

34 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 of access to their personal data (see question 14). This right includes the confirmation as to whether or not data relating to them is being processed and information at least regarding the purposes of the processing. Individuals may ask for incorrect or inadequate information to be rectified or deleted.

The Data Protection Law specifies that the right of access may be exercised free of charge, at reasonable intervals and without excessive waiting periods.

Any party who intentionally obstructs in any way the exercise of the right of access will be liable to a prison sentence of between eight days and one year or a fine ranging between €251 and €125,000, or both of these penalties.

The PII owner is authorised to restrict or defer the exercise of a data subject's right of access, notably if such a measure is necessary in order to safeguard national security, defence or public safety.

35 Other rights

Do individuals have other substantive rights?

Data subjects can also ask the PII owner to rectify or delete data that is inaccurate or processed in breach of the Data Protection Law, free of charge (see question 14).

Data subjects can oppose, free of charge, the processing of their data, for legitimate reasons relating to their specific situation.

36 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 can bring civil actions before the courts in order to obtain damages. The claimant must show prejudice that must be direct, certain, personal and measurable.

37 Enforcement

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

In cases of illegal data processing, individuals are entitled to refer their case to the National Commission, which is entitled to prevent a data processing for non-compliance. The National Commission can also refer a case to the public prosecutor.

In order to claim for damages, individuals can also bring an action before the courts.

Exemptions, derogations and restrictions

38 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

39 Judicial review

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

The Data Protection Law gives the National Commission the power to impose administrative sanctions against the PII owner. These disciplinary sanctions have the legal nature of an administrative decision and, therefore, may be reviewed by the Administrative Court of the Grand Duchy of Luxembourg.

Specific data processing

40 Internet use

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

The Electronic Communication Law provides that the storage of information or the gaining of access to information already stored, in the terminal equipment of a subscriber or user, is only permitted if the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, inter alia, about the purposes of the processing. The Electronic Communication Law also expressly specifies that:

- the methods of providing information and offering the right to refuse must be as user-friendly as possible; and
- where it is technically possible and effective, the user's consent to processing may be expressed through appropriate browser or other application settings.

41 Electronic communications marketing

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

Both the E-Commerce Law of 14 August 2000 and the Electronic Communication Law of 30 May 2005 apply in respect of electronic communications marketing.

According to the E-Commerce Law of 14 August 2000, any provider must obtain prior consent from its potential customers before being able to send unsolicited commercial communications.

When providers obtain the electronic addresses of their customers through the sale of a product or a service, such providers may use these email addresses for commercial or marketing purposes and, notably, send commercial communications to such customers by electronic means. Providers, however, must allow their customers to oppose, free of charge, the use of their electronic address (see question 34).

Customers must be able to oppose such use at the time of the collection of their email address and during the reception of any new commercial communications.

Any unsolicited electronic commercial communication must comply with the following conditions:

- the commercial communication must be clearly identified as such;
- the provider who sends the commercial solicitation must be clearly identified; and
- competitions and promotional games must be clearly recognisable as such and their conditions of participation must be easily accessible and presented in a precise and unambiguous way.

In addition, the Electronic Communication Law prohibits the sending of electronic mails for the purpose of direct marketing while disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request for such communications to cease.

42 Cloud services

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

The CNPD has not issued any formal opinion on cloud computing guidance. Therefore, data protection issues arising from the deployment of cloud computing services are governed by the Data Protection Law, which shall be analysed in the light of opinions issued by the Article 29 Data Protection Working Party (Opinion on Cloud Computing WP 196, adopted 1 July 2012).

The law of 9 July 2013 has amended article 567 of the Commercial Code in order to adapt it to the new situations deriving from the latest technology developments, namely cloud computing. Article 567 of the Commercial Code, as amended, allows data subjects to claim their data in the case of bankruptcy of the provider or supplier (ie, a right of reversibility of data).

Marielle Stevenot **stevenot@mnks.com**
Rima Guillen **guillen@mnks.com**
Charles-Henri Laevens **laevens@mnks.com**

Vertigo Polaris Building, 2nd floor
2-4 rue Eugène Ruppert
L-2453
Luxembourg

Tel: +352 26 48 42 1
Fax: +352 26 48 42 35 00
www.mnks.com

Malta

Olga Finkel, Robert Zammit and Rachel Vella-Baldacchino

WH 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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Malta enacted the Data Protection Act in 2001 (the Act). This, together with a number of pieces of subsidiary legislation, forms the local legislative framework for the protection of PII. The Constitution of Malta also provides for the protection of the fundamental rights and freedoms of individuals, which provides constitutional protection to the respect of privacy of every person's home and family life.

Malta is a party to the Universal Declaration of Human Rights, to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Malta is also a member of the European Union and consequently is bound to adhere to all EU directives, regulations and recommendations including Directive 95/46/EC.

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 the implementation of data protection law is the Office of Information and Data Protection Commissioner (the Commissioner). The Commissioner has a number of functions, which include, but are not limited to:

- creating and maintaining a public register of all processing operations according to notifications submitted;
- exercising control and verifying whether processing is being carried in accordance with the Act and the regulations;
- issuing directions and guidelines;
- instituting civil legal proceedings in case of breach of the Act and referring any criminal offence encountered in the course of this function to competent authorities;
- ordering the blocking, erasure or destruction of data, or imposing a temporary or permanent ban on processing, or warning or admonishing controllers; and
- at the request of data subjects, verifying that the processing of data is compliant with the Act.

As part of the investigative powers of the Commissioner, the Commissioner is entitled to obtain access to personal data that is being processed and information about, and documentation of, the processing of personal data and the security of such processing upon request. In exercising this function the Commissioner is empowered to enter and search any premises under the powers that are vested in executive police by any law.

3 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 particular provisions of the Act may lead to criminal penalties, which vary from fines of €120 up to €23,300 and imprisonment of not more than six months. The criminal penalties may vary depending on the provisions of the Act being breached. On encountering a breach of the Act, which could lead to criminal proceedings, the Commissioner is to refer the situation to the competent authorities who in turn would need to take action in the Criminal Courts of Malta.

Other breaches of the Act may result in administrative fines, which can vary from one-time fines of up to €23,300 and daily fines of up to €2,500, depending on the provisions of the Act being breached.

Scope

4 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 Act does not apply to the processing of personal data where such processing is undertaken by a natural person in the course of a purely personal activity and to processing operations concerning public security, defence, state security (which includes economic well-being of the state when the processing operation relates to security matters) and activities of the state in areas of criminal law.

5 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 Act covers direct marketing. However interception of communications, unsolicited communications over electronic communications and the monitoring and surveillance of individuals are covered by the Processing of Personal Data (Electronic Communications Sector) Regulations 2003, which implement the provisions of Directive 2002/58/EC and Commission Regulation 611/2013. Interception of communications is also covered by the Electronic Communications Networks and Services (General) Regulations, subsidiary legislation 399.28 and by the Security Service Act, Chapter 391 of the Laws of Malta.

6 Other laws

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

Under the Act a number of subsidiary legislations have been enacted.

- The Processing of Personal Data (Protection of Minors) Regulations provide for permitted processing in the case of any information obtained by a teacher or any other person acting in loco parentis or in his or her professional capacity in relation to a minor if such processing is in the best interest of the minor.

- The Data Protection (Processing of Personal Data in the Police Sector) Regulations are to ensure a high level of data protection in the police sector and any other public body exercising police powers.
- The Processing of Personal Data (Police and Judicial Cooperation in Criminal Matters) Regulations have been enacted to ensure a high level of protection of fundamental rights and freedoms of natural persons.

7 PII formats

What forms of PII are covered by the law?

The Act covers the processing of personal data as well as sensitive personal data. The Act defines personal data as any information relating to an identified or identifiable natural person, whereby an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Sensitive personal data is defined as personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health or sex life.

8 Extraterritoriality

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

The territorial scope of the Act is limited to the processing of personal data in Malta or in a Maltese Embassy or High Commission abroad, and to the processing of personal data where the controller is established in a third country but the equipment used for processing is located in Malta, except where the equipment is only used for the purpose of transmitting information.

9 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?

The act of processing PII is defined broadly in the Act to cover any operation or set of operations that is taken in regard to personal data, whether or not it occurs by automatic means and includes the collection, recording, organisation, storage, adaptation, alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction of such data.

Different responsibilities are placed on the controller of the personal data and the processor, who processes personal data on behalf of a controller. The processor is not allowed to process personal data other than in accordance with instructions from the controller, unless there is a legal requirement. Furthermore, the Act requires that the processing by a processor is to be done under a written contract whereby the processor is bound to act only on the instructions of the controller and to ensure that the required security measures relating to processing are in place.

Legitimate processing of PII

10 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 article 9 of the Act, personal data may be processed only in the circumstances below:

- the data subject has given unambiguous consent; or
- processing is necessary for:
  - performance of a contract to which data subject is a part to or in order to take steps at the request of the data subject prior to entering into a contract;
  - compliance with a legal obligation to which the controller is subject;
  - protection of the vital interests of the data subject;
  - the performance of an activity that is carried out in the public interest; or
  - a purpose that concerns a legitimate interest of the controller or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy.

11 Legitimate processing – types of PII

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

The Act specifies that sensitive personal data may not be processed unless explicit consent is obtained from the data subject or the data subject has made the sensitive personal data public.

Furthermore, the Act provides that sensitive personal data may be processed if appropriate safeguards are adopted and the processing is necessary in order that the controller will be able to comply with his or her duties as an employer, or it will be possible to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving his or her consent, or it will become possible to establish, exercise or defend legal claims.

The Act further provides that there are other situations where sensitive personal data may be processed.

These include when the processing of sensitive data is done:

- on the members of a body of persons or other entity not being a commercial body, with political, philosophical, religious or trade union objects in the course of its legitimate activities with appropriate guarantees, by the mentioned body of persons;
- for health and hospital care purposes, provided that it is necessary for preventive medicine and the protection of public health; medical diagnosis; health care or treatment; or management of health and hospital care services; and
- for research and statistics purposes, provided that processing is necessary for the performance of an activity that is carried out in the public interest.

The processing of sensitive personal data for research and statistics purposes may also be done in the case of statistics, with Commission approval; and in case of research, also with Commission approval, on the advice of the research ethics committee of an institution recognised by the Commissioner.

In the absence of consent, a legally valid identification document may only be processed when such processing is clearly justified having regard to the purpose of the processing, secure identification or some other valid reason as may be prescribed.

Data relating to offences, criminal convictions or security measures may only be processed under the control of a public authority unless specifically provided for under any other law.

Data handling responsibilities of owners of PII

12 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 owners of PII must provide the individuals whose data they hold with:

- the identity and habitual residence or principal place of business of the owner of PII and of any other person authorised by him or her to process data;
- the purpose of processing;
- any further information relating to the recipients or categories of the recipients of data;
- whether the reply to any question made to the data subject is obligatory or voluntary; and
- the existence of the right to access, the right to rectify and the right to erase the data.

This information must also be provided in the situation where the data collected was collected from other sources.

Such information needs to be provided at the time of undertaking the recording of the personal data, or when the information is obtained from other sources, not later than the time when the data is first disclosed.

13 Exemption from notification

When is notice not required?

The information does not need to be provided where the data subject already has this information, and where the processing is for statistical purposes or for historical or scientific research, or if there are provisions in any other law and adequate safeguards are adopted.

14 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 the individuals whose data is held by owners of PII, the owners of PII are required to provide written information as to whether personal data concerning the data subject is held, without excessive delay and without expense.

It should be noted that such requests for information on the data held by the owners of PII should only be made at reasonable intervals.

The owners of PII should inform the individual what information is being processed, where the information was collected, the purpose of the processing, to whom the information has been disclosed and knowledge of the logic involved in any automatic processing of data concerning the individual.

The owner of PII is required to immediately rectify, block or erase personal data on the request of the individual in accordance with the law.

The owner of PII is also obliged to provide data subjects about their right to opt out from direct marketing, and must provide easy and simple opt-out methods free of charge. Data subjects who want to opt out must give notice to the owner of PII that they oppose such processing of their data. Direct marketing via non-electronic means can be provided unless the data subject has opted out from receiving such marketing; direct marketing via electronic means requires an opt-in unless the data subject is a customer of the owner of PII and the direct marketing is related to the latter's own products and services (details of opt-out methods must be sent to the data subject in each and every message).

15 Data accuracy

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

The owner of PII is required by law to ensure that personal data is processed fairly and lawfully. The owner of PII is also required to ensure that personal data is adequate and relevant in relation to the processing as well as correct and if necessary, up to date. The owner of PII must take all reasonable measures to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, taking into account the purpose for which the data is processed.

16 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 information is not to be kept for a period longer than is necessary, having regard to the purposes for which it is processed. This would mean that if information is obtained in the creation of a business relationship, then one would look into the prescriptive period in which a claim may be made following the termination of the relationship and such period would be the maximum period that the owner of PII is allowed by law to keep that information.

17 Finality principle

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

Yes. The owner of PII must ensure that personal data is only collected for specific, explicitly stated and legitimate purposes. Furthermore, no more personal data is to be processed than is necessary.

18 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 cannot be processed for any purpose other than that explicitly stated. This means that if the owner of PII is to process it for some other purpose, he or she would need to get explicit consent, unless one of the other grounds for processing applies.

Security

19 Security obligations

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

The law provides that the owners of PII are to implement technical and organisational measures appropriately to protect the personal data from accidental destruction, loss or unlawful forms of processing.

Adequate security should be in line with what is technically possible and normal costs of implementing security measures that mitigate the special risk that exists in the processing of sensitive personal data. Thus the owners of PII are allowed some discretion in implementing the security measures that they consider sufficient in their circumstances.

Where PII is processed by third-party service providers, the owner or controller of the data must ensure that the outsourced processor adopts security measures that are no less stringent than the requirements that are applicable to it in terms of the DPA. The owner bears the ultimate responsibility to identify that the service provider has the capacity of implementing the necessary security measures and for seeing that these measures are actually carried out.

20 Notification of data breach

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

Presently, there is no general requirement under the Act that obliges the owner of PII to notify the regulator or the individual on whom information is collected that a breach of security ensued.

However, the data controllers are required to submit to the Commissioner requests for processing of personal data that involve particular risks of improper interference with the fundamental rights and freedoms of data subjects.

Where the data controller is a provider of publicly available electronic communications services he or she is required to notify the Commissioner of a personal data breach without undue delay. If the breach is likely to also affect the personal data or privacy of an individual, the owner of PII must notify the individual of the breach without undue delay. Notifying the individual is not required if the owner of PII has demonstrated to the satisfaction of the Commissioner that he or she has implemented appropriate technological protection measures, such that the data is rendered unintelligible to unauthorised individuals and that those measures were applied to the data concerned by the security breach.

Notifying the individual shall at least include the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach.

Notifying the Commissioner shall, in addition, include the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

Internal controls

21 Data protection officer

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

It is mandatory to appoint a representative established in Malta when the owner of PII is established in a third country and the equipment used for processing is situated in Malta. There is no other mandatory requirement to appoint a data representative. However, if a data representative is appointed he or she shall have an independent role and is required to

ensure that the owner of PII processes the personal data in a lawful and correct manner, and in accordance with good practice. The data representative is only bound to inform the owner of PII should he or she notice any inadequacies.

The personal data representative is obliged to report to the Commissioner if there is any suspicion that the owner of PII has contravened the provisions for processing and no rectification was implemented after the personal data representative informed the owner of PII of the situation.

The personal data representative is an independent function and is required to consult with the Commissioner in the event of doubt about how the rules applicable to processing are to be applied.

22 Record keeping

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

Owners of PII are legally obliged to process personal data in line with the principles established by the Act and to ensure that they are adequately protecting that personal data throughout its lifecycle, from collection to use, to disclosure and to destruction. It is of utmost importance that the owner of PII effectively manages the personal data that he or she collects and processes.

Although the Act does not specifically state this, in addition to technical and physical measures to protect personal data, owners of PII must take the necessary administrative measures. These safeguards include measures such as company policies, training, procedures, privacy notices (ie, external statements) to ensure the proper management of privacy and security of customer and employee personal data.

The proposed Draft Data Protection Regulation currently includes documentation obligations on data controllers – as well as the appointment of a personal data representative if the organisation legally qualifies for one – therefore it would be wise for data controllers to start preparing for this. In case of a breach, the company would need to show that it took all the necessary steps (technical, administrative and physical) it could take to keep the personal data safe and secure and that it acted in a responsible manner throughout. Moreover, the Commissioner can carry out an on-site investigation to make sure that the company did in fact take all these measures.

Registration and notification

23 Registration

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

Yes, owners and processors of PII are to register with the Commissioner. The notification should be made before carrying out any wholly or partially automated or manual processing operation.

The Commissioner may allow the simplification of, or the exemption from, notification obligation only in respect of processing operations that are unlikely to prejudice the rights and freedoms of data subjects, and in respect of which the Commissioner specifies the purposes of the processing, the data or categories of data being processed, the category or categories of data subjects affected by such processing, the recipients or categories of recipients to whom the data is to be disclosed and the length of time for which the data is to be stored.

24 Formalities

What are the formalities for registration?

The notification is to be submitted before carrying out any processing operation and should include:

- the name and address of the data controller and of any other person authorised by him or her;
- the purpose or purposes of processing;
- a description of the category of data subject and of the data relating to them;
- the recipients to whom data might be disclosed;
- proposed transfers of data to third countries; and
- a general description allowing preliminary assessment to be made of the appropriateness of the security measures taken.

Unless the data provided in the first notification changes, the owner of PII is not required to resubmit any documentation.

A fee of €23.29 is payable on a yearly basis, where the year runs from July to June.

25 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 Commissioner may impose an administrative fine if the data controller fails to notify the Commissioner when data processing begins, and the fine shall be considered a civil debt. This administrative fine can vary between €120 and €600, in addition to a daily fine, which can be between €20 and €60.

26 Refusal of registration

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

The Act is silent on refusal of entry on the register as a data controller or personal data representative. The obligation is on the owner of PII to submit the necessary form and fee to be so registered. In case of breach of such an obligation, the Commissioner may impose certain restrictions on the owner of PII, such as a temporary ban on processing and may also admonish, issue warnings and impose fines.

27 Public access

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

The register of data controllers and personal data representative is public and is available online on the website www.idpc.gov.mt.

28 Effect of registration

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

There is no specific legal effect on entry on the register, as once data processing begins, the data owner or processors are bound by the requirements of the law.

Transfer and disclosure of PII

29 Transfer of PII

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

The owner of PII may appoint third parties to process data. Such third parties may only process the personal data in accordance with the instructions of the owner of PII, unless the third party is otherwise required to do so by law. A written agreement is required for the appointment of third party providers to provide processing services. The agreement should provide instructions from the owner of PII and the technical and organisational measures that the controller implements to protect the personal data, so that the service provider follows the same measures. It is the responsibility of the owner of PII to ensure that third party providers can implement such measures and do so.

30 Restrictions on disclosure

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

As long as the owner of PII has obtained explicit consent from the data subject to disclose the PII to other recipients, and it is made clear what the purpose of the disclosure is, then there are no other restrictions on disclosure of PII to other recipients.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Transfer of PII outside the jurisdiction is allowed for as long as the jurisdiction whereto the transfer of PII is to occur has adequate levels of protection of data. It is at the Commissioner's discretion whether or not a third country has adequate levels of data protection, as the owner of PII is required to obtain the Commissioner's approval to transfer PII outside of the jurisdiction.

The law further specifies that transferring to a third country that does not have the adequate levels of protection is prohibited. Nevertheless, it is

Update and trends

An emerging issue in Malta is the recent adoption by the European Parliament and the Council in April 2016 of the EU's new General Data Protection Regulation, which will affect entities that in some way process, control or handle personal data. The new rules encourage businesses to adopt privacy-friendly data techniques such as anonymisation, pseudonymisation and encryption, and will provide a level playing field for all EU and non-EU businesses, as all entities providing services to EU consumers and data subjects must comply with these rules. Typically, EU regulations come into force after 20 days from their original publication in the Official Journal of the EU. However, businesses are not going to be subject to the new rules just yet and are to be allowed a two-year grace period. During this time, data controllers are strongly advised to allocate the time and resources necessary to ensure compliance with the new data protection rules, once they come into force in 2018.

allowed to transfer to a third country that does not have adequate levels of protection if the Commissioner is satisfied that the controller will provide adequate safeguards, such as clear contractual obligations with the service provider in the third country. In analysing whether the agreements with the service provider are sufficient, the Commissioner should consider the provisions of Commission Decision 2001/497/EC of 27 December 2004 and Commission Decision 2010/87/EU of 5 February 2010.

Moreover, such transfer is also allowed if the transfer is necessary for the performance of a contract, or is necessary or legally required on public interest grounds, or for the establishment, exercise or defence of legal claims, to protect the vital interests of the data subject. In addition, transfer may be effected to a third country where there is no adequate level of protection if it is made from a register that according to laws is intended to provide information to the public.

It is to be noted that any country that is a member of the European Union, the European Economic Area (EEA) or a third country or jurisdiction that is not a member of the EU or the EEA but is from time to time recognised by the EU commission to have an adequate level of protection (currently Andorra, Argentina, Australia, Canada, Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay), and organisations complying with the US Department of Commerce's Safe Harbor Privacy Principles, are not considered as third countries, therefore transfer to these jurisdictions is allowed and does not require authorisation from the Commissioner.

32 Notification of cross-border transfer

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

The owner of PII is required to notify the Commissioner where international data transfer is to be made by submitting a form. Where the transfer of data is to be made to a third county, the approval of the Commissioner is required prior to such transfer being made.

33 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 for transfer of data to a third country hold irrespective of whether the transfer is to be made to a service provider or to other data owners.

Rights of individuals

34 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 law provides that the individual has the right of access; however, the right does not include the right to see a copy of their personal information held by PII owners. The PII owner is required, however, to provide in written form to the individual actual information about the data subject that is processed, where the information has been collected, the purpose of the processing and to which recipients the information is disclosed. The PII owner is also required to provide in writing an explanation of the logic involved in any automatic processing of data concerning the individual.

The individual must make such a request in writing. This cannot be made frequently, but should be done at reasonable intervals.

35 Other rights

Do individuals have other substantive rights?

Under the Act, data may not be processed for direct marketing, unless the individual has given his or her explicit consent. The individual, however, has the right to oppose the processing of his or her data for the purpose of direct marketing at no cost.

The individual also has the right to rectify, and where applicable, the right to erase the data concerning him or her. It is the duty of the owner of PII to immediately rectify, block or erase personal data that is not being processed in accordance with the Act.

36 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 sue any owner of PII who has processed data in contravention of the Act for damages, by filing a sworn application with the competent court. Under Maltese law, there has to be actual damage for there to be compensation.

37 Enforcement

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

Actions for damages are to be filed with the competent courts. However, individuals may apply for the Commissioner to take adequate action against the owners of PII, should they feel that there was a breach of the Act.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

The principles of data protection, the requirement to provide the individual with certain information, the right to access and the maintenance by the Commissioner of a register of processing operations shall not apply when the law specifically provides that processing the data is a necessary measure in the interests of:

- national security, defence or public security;
- prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions;
- economic or financial significance, including monetary, budgetary and taxation matters;
- monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority; or
- such information that is prejudicial to the protection of the individual or of the rights and freedoms of others.

Supervision

39 Judicial review

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

Data owners may appeal to the Information and Data Protection Appeals Tribunal. This Tribunal is formed of a chairman and two other members appointed by the minister responsible for freedom of information and data protection. The appeal has to be filed within 30 days from the decision of the Commissioner.

The grounds for an appeal to the Tribunal are limited to material error on the facts of the case, material procedural error, error of law, or material illegality, including unreasonableness or lack of proportionality.

A party may furthermore appeal a decision of the Tribunal with the Court of Appeal on questions of law.

Specific data processing

40 Internet use

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

The Processing of Personal Data (Electronic Communications Sector) Regulations implements the amended European Commission Directive 2009/136/EC, better known as the e-Privacy Directive. To this effect, the use of cookies is prohibited, except in limited circumstances where the user has opted in to their use.

Due to the controversy surrounding the e-Privacy Directive, the Article 29 Data Protection Working Party was established to develop guidelines for owners of PII in relation to the use of cookies. The guidelines establish that owners of PII who operate a website should ensure that consent is obtained before the use of cookies and that such consent should be specific, unambiguous and freely given. The Office of the Commissioner in Malta has decided to follow the guidelines issued by the Working Party, which means that any owner of PII in Malta is required to ensure that these requirements are followed when using cookies.

41 Electronic communications marketing

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

The Act provides that direct marketing is only allowed if the individual has given his or her consent. However, the Processing of Personal Data (Electronic Communications Sector) Regulations provide that an owner of PII shall not use, or cause to be used, email, fax or telephone for the purpose of direct marketing unless the individual has given prior consent in writing. Having said that, if the contact details were obtained in relation to the sale of a product or a service, it is allowed to use email for marketing purposes for similar products or services.

The owner of PII is, however, required at the time of collection to give the opportunity to the individual to object, free of charge and in an easy and simple manner, to such use of the email details.

It is forbidden to send email for direct marketing whereby the identity of the sender is disguised or concealed.

42 Cloud services

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

Maltese regulatory authorities have thus far not issued guidance or rules that specifically address the use of cloud computing services. At present, cloud computing raises data protection concerns under Maltese data privacy law when the data is hosted on cloud servers that are located outside of the EU, in which case the transfer of data must be notified to the Commissioner and approved in the same manner as other third-country data transfers (see question 32).

Current policy frameworks seek to mitigate risks, while at the same time seizing the full benefits of cloud computing. This can be seen, for instance, in the licensing approach carried out at present by the Malta Gaming Authority, Malta's public regulatory body responsible for all forms of gaming, where requests for use of public or private cloud are dealt with on a case-by-case basis during the licensing process of a remote gaming operator. The same approach is to be seen with respect to financial services licence applications before the Malta Financials Services Authority (the single regulator of financial services in Malta).

wh·partners
ADVOCATES & SOLICITORS

Olga Finkel **olga.finkel@whpartners.eu**
Robert Zammit **robert.zammit@whpartners.eu**
Rachel Vella-Baldacchino **rachel.vellabaldacchino@whpartners.eu**

Level 5 Quantum House
75 Abate Rigord Street
Ta' Xbiex XBX1120
Malta

Tel: +356 209 251 00
Fax: +356 209 259 02
www.whpartners.eu

Mexico

Gustavo A Alcocer and Abraham Díaz Arceo
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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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 Data Held by Private Parties, published in July 2010, its Regulations, published in December 2011, the Privacy Notice Rules, published in January 2013, and the Binding Self-Regulation Parameters, also published in January 2013 and May 2014. Mexican PII protection law 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), thus providing several rights to individuals and obligations to PII controllers 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 the individuals' right to privacy. INAI has the authority to conduct investigations, review and sanction PII controllers, 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 INAI.

3 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, depending on the seriousness of the breach and specific behaviour and conduct that may lead to criminal penalties is sanctioned from three months and up to 10 years imprisonment, depending on the seriousness of the breach (profit-making with PII or the methods used to get consent for the use of the PII) and 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 breach and illegal access to media systems and equipment.

Scope

4 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 only 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 bureaus 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.

5 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 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 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 Consumer's Protection sanctions the publication in any massive media of any notice addressed undoubtedly to one or various specific consumers, with the aim of collecting a debt from them, or having them to comply with an agreement.
- Article 76-bis of the Federal Law for Consumer's 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.

6 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 and the Law for the Regulation of Credit Information Companies, there is additional legislation covering specific data protection rules, such as the Civil Code, and the Code of Commerce.

7 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 only accessed 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).

8 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.

9 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?

Yes, 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 owners, 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.

Legitimate processing of PII

10 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 ('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.

11 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 (ie, 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

12 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.

The privacy notice should contain at least the following information:
- the identity and address of the PII controller;
- the purpose of the processing;
- the mechanisms provided by the PII controller to the individuals to limit the use or disclosure of the information;
- 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 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 new 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 check marks in text boxes, these must not be pre-checked; and
- reference to texts or documents not available to individuals must be omitted.

13 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.

14 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 PII controller correct the PII that is incorrect or inaccurate), cancel (the right to request the PII to stop treating their PII) or oppose (the right to refuse the processing of their PII) the processing of their PII.

15 Data accuracy

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

As discussed in question 10, 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.

16 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.

17 Finality principle

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

As discussed in question 10, 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.

18 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

19 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 on the PII and the systems used for its in 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.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and 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.

Internal controls

21 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.

22 Record keeping

Are owners 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.

Registration and notification

23 Registration

Are PII owners and/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 the PII controllers are complying with the Law and Regulations.

24 Formalities

What are the formalities for registration?

Not applicable.

25 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.

26 Refusal of registration

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

Not applicable.

Update and trends

In June 2016, the Mexican Supreme Court of Justice confirmed the constitutionality of article 190 of the Federal Telecommunications and Broadcast Law, which allows Mexican investigative authorities to request the geolocation of a mobile phone, or electronic device in real time, without previously obtaining a judicial order.

Likewise, the Mexican Supreme Court of Justice confirmed the constitutionality of the obligation of telecommunication companies, to store all of their client's big data, for a time period of 24 months. This big data includes, among others: list of phone calls; dates and hours of the calls; digital and satellite locations; and payment modalities.

The rationale behind this decision is that the Supreme Court considered that geolocation does not imply an intrusion to privacy, since it is only aimed at identifying the location of a phone call, but it is not aimed at locating a specific and identifiable person.

27 Public access

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

Not applicable.

28 Effect of registration

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

Not applicable.

Transfer and disclosure of PII

29 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 transfer of PII as the communication of PII to third parties, whether inside or outside Mexico, other than from the PII controller, the officer in charge or the service provider (PII controlling company).

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.

30 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.

31 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, health care 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.

Cross-border PII transfer is allowed as long as such transfer is made by written agreement (or similar) detailing all the conditions under which the PII controller received the PII, as well as a description of each party's obligations and the purpose of the transfer. The receiving party will have the same obligations as a PII controller and it will be considered as such.

32 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.

33 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

34 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 35) 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.

35 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.

36 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?

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.

37 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

38 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

39 Judicial review

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

Yes. Since INAI is an administrative authority, any of its resolutions can be challenged through a nullity trial before the Federal Court for Tax and Administrative Affairs, and later on through a Constitutional rights action known as *Amparo* suit.

OLIVARES

Gustavo A Alcocer **gustavo.alcocer@olivares.mx**
Abraham Díaz Arceo **abraham.diaz@olivares.mx**

Pedro Luis Ogazón 17
Col. San Angel
01000 Mexico City
Mexico

Tel: +52 55 53 22 30 00
Fax: +52 55 53 22 30 01
www.olivares.com.mx

Specific data processing

40 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, which allow them to collect PII automatically and simultaneously at the same time that individuals have contact with such PII, 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.

41 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.

42 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.

The guidelines have not been issued yet to regulate the processing of PII in cloud computing.

Poland

Arwid Mednis and Gerard Karp
Wierzbowski Eversheds

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The Polish Personal Data Protection Act of 29 August 1997, (PDPA) is the primary legislation concerning data protection in Poland. The PDPA is the adoption of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The European Convention on Human Rights and Fundamental Freedoms was ratified in 1993. The European Court of Human Rights has jurisdiction over the cases of Convention breaches.

In 2002 Poland also ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

There are eight executive regulations issued on the basis of the PDPA, including the Regulation of 29 April 2004 by the Minister of Internal Affairs and Administration (the Regulation) as regards personal data processing documentation and technical and organisational conditions that should be fulfilled by devices and computer systems used for personal data processing.

2 Data protection authority

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

The Polish data protection authority is the Inspector General for Data Protection (DPA). The DPA's duties include:

- supervising conformity of data processing with the personal data protection legislation;
- issuing administrative decisions and reviewing complaints in cases involving enforcement of the personal data protection legislation;
- ensuring that non-monetary obligations arising from the issued decisions are performed by the obligees by applying the enforcement measures provided for in the Regulation; and
- maintaining a register of filing systems and providing information on the registered filing systems.

The DPA, as well as the authorised employees of the DPA's bureau, to properly supervise data processing and ensure that all legal obligation relating to personal data processing are fulfilled, may:

- access premises in which data is processed;
- request written or oral explanations and summon and interrogate persons insofar as may be necessary to determine the facts;
- review any documents and any data directly associated with the subject matter of the inspection and make copies thereof;
- inspect devices, media and computer systems used for the processing of data; and
- request expert opinion and evaluation.

3 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 violation of rules stipulated by the PDPA (and other statutory, if applicable) may result in both administrative and criminal liability.

The authority responsible for compliance of data processing with the provisions on the protection of personal data is the DPA.

The DPA may issue a decision requiring the data controller to cease processing and delete the personal data collected. It may also impose an administrative fine in case of non-compliance with the decision.

The PDPA contains criminal sanctions for a data controller that illegally processes data, including fines, restrictions of personal liberty or imprisonment for up to three years.

Criminal proceedings are handled by the prosecutor's office.

Also, under Polish Civil Code, unlawful processing may be subject to a civil lawsuit.

Scope

4 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 provides for certain exceptions, (ie, there are entities or areas of activity to which it does not apply). These exceptions are:

- natural persons involved in the processing of data exclusively for personal or domestic purposes;
- entities having their seat or residing in a third country that use technical means located within the territory of the Republic of Poland exclusively for the transfer of data;
- press journalistic activity within the meaning of the Act of 26 January 1984 – the Press Law – and literary and artistic activity, unless the freedom of expression and information dissemination considerably violates the rights and freedoms of the data subject (however, provisions of the PDPA regarding the supervision and competences of the DPA, as well as the provisions specifying the security obligations of the data controller still apply); and
- any cases where an international agreement to which the Republic of Poland is a party provides for otherwise.

If any separate laws on the processing of data provide for more extensive protection of the personal data than the provisions of the PDPA, then the provisions of such laws providing more extensive protection take precedence. This does not mean that the PDPA will not apply in any matters unregulated by such laws.

5 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 and executive regulations do not wholly cover interception of communications, electronic marketing or monitoring and surveillance of individuals. Relevant laws in this regard are:

- the Act of 16 July 2004 – the Telecommunications Law (TL);
- the Act of 18 July 2002 on Electronically Supplied Services (ESSA); and
- the Act on Visual Monitoring (which is currently only a draft making its way through the legislation procedure, so it is impossible to estimate when the it will enter into force).

6 Other laws

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

The most important regulations that provide specific data protection rules are those regarding: banking law, labour law, regulations on employee documentation, regulations on medical documentation, insurance law, capital markets law, payment services, statistical information and record-keeping, and regulations regarding civil and national security (eg, concerning the police, foreigners, criminal records, mass events, the Central Anti-Corruption Bureau).

7 PII formats

What forms of PII are covered by the law?

The PDPA applies to the following format of processing PII:

- files, indexes, books, lists and other registers; and
- computer systems, also in cases where data are processed outside from a data filing system.

It should be noted that, according to article 2 clause 3 of the PDPA, as regards personal data files that are prepared ad hoc, exclusively for technical, training, or higher education purposes, where the data are immediately removed or rendered anonymous after being used, only the provisions of the PDPA specifying security obligations apply.

8 Extraterritoriality

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

Applicability of the PDPA is extended beyond the territory of Poland. Namely, the PDPA applies also to natural and legal persons and organisational units not being legal persons who process personal data as part of their business or professional activity or the implementation of statutory objectives that have their seat or reside in a third country – if such processing of personal data is performed with the use of technical means located within the territory of the Republic of Poland.

9 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?

The PDPA constitutes the general and most important piece of legislation in the scope of personal data protection. It is only superseded by other laws to the extent that they provide for more detailed provisions.

The PDPA covers all processing and use of the PII. There is also a distinction between the data controller (ie, the person or entity who decides upon the purposes of means of personal data processing) and the data processor, who processes the personal data for and on behalf of the data controller, and on the basis of a written agreement. The data processor is not authorised to make decisions with regard to the purposes and means of the data processing. For detailed information on entrusting the personal data for processing, see question 30.

Legitimate processing of PII

10 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, Polish law requires that the holding of PII has specific legal ground for processing of personal data. Pursuant to article 23 of the PDPA, the processing of personal data is only permitted on the condition that one of the legal grounds listed in that provision applies. Those legal grounds are as follows:

- the data subject has given his or her consent, unless the processing consists of erasure of personal data;
- processing is necessary for the purpose of exercise of rights and duties resulting from a legal provision;
- 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;
- processing is necessary for the performance of tasks provided for by law and carried out in the public interest; or
- processing is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject.

Stricter grounds are stipulated for processing of sensitive personal data.

11 Legitimate processing – types of PII

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

Yes, Polish law imposes more stringent rules for processing of sensitive data (eg, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade union membership) as well as the processing of data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued in court or administrative proceedings. For example, processing of sensitive data shall not constitute a breach of PDPA where:

- the data subject has given written consent;
- processing relates to the data necessary to pursue a legal claim;
- provisions of the other statues allow processing of such data;
- processing is required for medical and health purposes;
- processing is necessary for employment issues;
- processing is to conduct scientific research including preparation of a thesis required for graduating from university or receiving a degree; and
- processing relates to personal data that were made publicly available.

Data handling responsibilities of owners of PII

12 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 law requires owners of PII to notify individuals about the fact that their data are being processed. Pursuant to article 24 of the PDPA, in cases where personal data are collected from the data subject, the controller is obliged to provide the data subject from whom the data are collected with the following information:

- the address of its seat and its full name, and, in case the controller is a natural person, about the address of his or her residence and his or her full name;
- the purpose of data collection, and, in particular, about the data recipients or categories of recipients, if known at the date of collecting;
- the existence of the data subject's right of access to his or her data and the right to rectify these data; and
- whether providing personal data is obligatory or voluntary, and in case of the existence of an obligation – about its legal basis.

Whereas, in cases where the data have not been obtained from the data subject, pursuant to article 25 of the PDPA, the controller is obliged to provide the data subject, immediately after the recording of his or her personal

data, all the information listed in the bullet points above and, additionally, of the source of data and the data subject's rights stemming from article 32 clause 1 point 7 and 8 (including the right to object to data processing).

13 Exemption from notification

When is notice not required?

In a case where personal data are collected from the data subject, the controller is not obliged to provide the data subject with the proper notice if:

- any provision of another law allows for personal data processing without disclosure of the real purpose for which the data are collected; or
- when the data subject already has the proper information (as described in question 12).

In a case where the personal data have not been obtained from the data subject, the controller is not obliged to provide the data subject with the proper notice if:

- the provision of another law provides or allows for personal data collection without the need to notify the data subject;
- the data are necessary for scientific, didactic, historical, statistical or public opinion research, the processing of such data does not violate the rights or freedoms of the data subject, and the fulfilment of the terms and conditions for providing the proper notice would involve disproportionate efforts or endanger the success of the research;
- the data are processed by the PII on the basis of legal provisions; and
- the data subject already has the proper information.

14 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, the owners of PII are obliged to ensure individuals exercise their statutory rights. Data subjects may: withdraw previous consent to processing; object to the processing of their personal data; ask for incorrect or incomplete data to be corrected or updated; and in some situations can take action to prevent further processing or to claim damages for breach of the legislation. Moreover, in the event of processing personal data that is collected indirectly (ie, from a source other than the data subject), the person to whom the personal data relates is entitled to object to data processing.

Rights of the data subject in the above scope are regulated in article 32 of the PDPA. According to that provision, the data subject has a right to control the processing of his or her personal data contained in filing systems, and in particular he or she has the right to:

(i) demand the data be completed, updated, rectified, temporarily or permanently suspended or erased, in case they are not complete, outdated, untrue or collected with the violation of the PDPA, or in case they are no longer required for the purpose for which they have been collected; and

(ii) make a justified demand in writing, in cases referred to in article 23 clause 1 point 4 and 5 of the PDPA (ie, processing necessary for the performance of tasks provided for by law and carried out in the public interest or processing necessary for the purpose of the legitimate interests pursued by the controllers or data recipients), for the blocking of the processing of his or her data, due to his or her particular situation.

It should be underlined that, under the PDPA, in the case that the data subject objects to the processing of his or her data, as referred to in (ii), the data controller is obliged to immediately stop the processing of the questioned data or without undue delay transmit the demand to the Inspector General, who shall make an appropriate decision.

15 Data accuracy

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

Yes, article 26 of the PDPA imposes standards on the quality, currency and accuracy of PII. A data controller is under an obligation to ensure that the personal data it is collecting, purchasing or otherwise retaining is relevant, adequate and not excessive for the purposes for which it will be used. For example, if the sole reason for obtaining the personal data of an individual data subject is to contact them about a job application they have made, the company will only need very limited details about them and may not be able to justify at that stage collecting details of their health and fitness. Moreover, personal data should not be collected and used or stored on an individual, unless it has a purpose for which the data subject has, where necessary, been fairly notified and that can be justified.

16 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, as determined in question 15, the owner of PII is obliged to collect only data that is relevant and adequate for the purposes of processing. Regarding the length of time data may be held, there are no particular provisions regulating that matter. Article 26, section 1, subsection 4 of the PDPA stipulates only that the data controller should ensure that the data are kept no longer than is necessary for the purpose for which it is processed.

17 Finality principle

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

On the basis of article 26 of PDPA, the owners of PII performing the processing of data should protect the interests of data subjects with due care, and in particular ensure that the data are collected for specified and legitimate purposes and not further processed in a way that is incompatible with the intended purposes.

18 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, provided that it does not violate the rights and freedoms of the data subject and is done:

- for the purposes of scientific, didactic, historical or statistical research;
- subject to the provisions of article 23 and article 25 of the PDPA (ie, on the basis of the one of the legal grounds described in question 10 and subject to notification of the data subject, as described in question 12).

Security

19 Security obligations

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

The Regulation imposes a technical and safety obligation while processing personal data, on both the controller and the processor. The requirements include:

- the requirement to assess the required security level out of the three available (basic, medium, high);
- 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 small and capital letters, numbers and special characters; and
- the requirement to apply cryptographic protection measures for the data used for authentication that are being transferred on the internet.

20 Notification of data breach

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

The PDPA does not provide a general obligation of notification of security breach. Only entities providing telecommunication services are required to notify the DPA of any data security breach within three days, in compliance with the provision of the TL. Under the TL, additional obligations in case of any threat to the integrity of the telecommunications network may apply.

Internal controls

21 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 (DPO) is voluntary. If the DPO is appointed, the owner of PII must notify the DPA. The responsibilities of the DPO include:

- ensuring compliance with the provisions on the protection of personal data, in particular by:
  - checking compliance of personal data processing with the provisions on the protection of personal data and drawing up a report in this regard for the controller;
  - supervising development and update of the documentation referred to in article 36 paragraph 2 as well as supervising compliance with the principles specified in this documentation; and
  - ensuring that the persons authorised to process personal data become acquainted with the provisions on the protection of personal data; and
- keeping a register of data files processed by the controller.

22 Record keeping

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

Yes. If the owner of PII has appointed the DPO and notified the DPA, then he or she is obliged to keep a register of data files (with some exceptions, eg, files containing sensitive data). As mentioned in question 21, the DPO is responsible for keeping this register.

The owner of PII is required to establish the data security policy and the instruction of the management of the computer system processing personal data.

Registration and notification

23 Registration

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

The owner of PII is required to register the data filing systems with the DPA, unless he or she has appointed a DPO (if a DPO has been appointed, only the filing systems containing sensitive data have to be registered with the DPA).

The obligation to register data filing systems does not apply to the owners of data that:

- contain classified information;
- were collected as a result of inquiry procedures held by officers of the bodies authorised to conduct such inquiries;
- are processed by relevant bodies for the purpose of court proceedings and on the basis of the provisions on National Criminal Register;
- are processed by the Inspector General of Financial Information;
- are processed by relevant bodies for the purposes of the participation of the Republic of Poland in the Schengen Information System and the Visa Information System;
- are processed by competent authorities on the basis of the provisions on exchange of information with prosecuting bodies of member states of the European Union;
- relate to the members of churches or other religious unions with an established legal status, being processed for the purposes of these churches or religious unions;
- are processed in connection with employment by the controller or providing services for the controller on the grounds of civil law contracts, and also refer to the controller's members and trainees;
- refer to the persons availing themselves of their healthcare services, notarial or legal advice, patent agent, tax consultant or auditor services;
- are created on the basis of electoral regulations concerning the Diet, Senate, European Parliament, communal councils, poviat (county) councils and voivodship regional assemblies, the President of the Republic of Poland, head of the commune, major or president of a city elections, and the acts on referendum and municipal referendum;
- refer to persons deprived of freedom under the relevant law within the scope required for carrying out the provisional detention or deprivation of freedom;
- are processed for the purpose of issuing an invoice, a bill or for accounting purposes;
- are publicly available;
- are processed to prepare a thesis required to graduate from a university or be granted a degree;
- are processed with regard to minor current everyday affairs; and
- are processed in data files that are not kept with the use of IT systems, except for the files containing sensitive data.

The processors of PII are not obliged to register the data filing systems with the DPA.

24 Formalities

What are the formalities for registration?

The motion concerning the data filing system submitted to the registration should contain the following:

- an application for entering the personal data filing system into the register of filing systems;
- specification of the controller and the address of its seat or place of residence, including an identification number from the National Official Business Register if such a number was granted, as well as the legal basis for maintaining the filing system and, in the case of entrusting data processing to the processor, or appointing a representative of the person having its registered seat in the third country, the specification of such entity and the address of its seat or place of residence;
- the purpose of processing the data;
- the description of the categories of data subjects and the scope of the processed data;
- information on the ways and means of data collection and disclosure;
- information on the recipients or categories of recipients to whom the data may be transferred;
- the description of technical and organisational security measures;
- information on the ways and means of fulfilling technical and organisational conditions specified in the Regulation; and
- information relating to a possible data transfer to a third country.

There is no fee required for registration. The Regulation provides the form of registration motion to be fulfilled by the owner of PII. The motion can also be submitted online.

25 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, fails to notify the data filing system for registration, is liable to a fine, the restriction of liberty or imprisonment for up to one year.

26 Refusal of registration

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

The DPA may refuse to register the data filing system if:

- the requirements specified in question 24 have not been fulfilled;
- the processing of data would breach the principles referred to in articles 23–28 (these provisions refer to the legal grounds of data processing, information obligation, adequacy and purpose limitation principle and the processing of sensitive data); and
- the devices and computer systems used for the processing of the data filing system submitted for registration do not meet the basic technical and organisational conditions defined in the Regulation.

27 Public access

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

Yes. It can be accessed in the DPA's office in Warsaw and online (https://egiodo.giodo.gov.pl/personal_data_register.dhtml).

28 Effect of registration

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

No, except for sensitive data. Such data can be processed once the DPA has issued a decision on the registration of the file.

Transfer and disclosure of PII

29 Transfer of PII

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

Under the PDPA, personal data may be transferred either to another, independent, data controller (disclosure of personal data) or to a data processor (entrusting the personal data for processing).

In case of the data processor, the transfer of the PII as such is not regulated. However, the PDPA provides for specific requirements in the scope of the agreement that the data controller needs to conclude with the data processor.

30 Restrictions on disclosure

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

When PII is disclosed to a service provider (data processor), then this is referred to as 'entrusting the data for processing'. In order for such disclosure (and further operations of the processor) to be legitimate, specific requirements stipulated in the PDPA need to be complied with. Otherwise, the processor may be considered to constitute an independent data controller, and, consequently, be found not to act in compliance with the PDPA (eg, by not fulfilling all of the data controller's obligations under the act).

An agreement on entrusted data processing must be executed in writing and state the scope and purpose of data processing. It may form part of a larger agreement (eg, laying down general conditions of cooperation).

The data processor is responsible for ensuring appropriate security measures for data processing, which are laid down in articles 36–39 of the PDPA, as well as adhering to security requirements specified in the Regulation. In the context of complying with security requirements mentioned above, the data processor bears liability as does the data controller (the processor's regulatory obligations). Apart from that, the processor is liable for acting in compliance with the agreement on entrusted data processing (the processor's contractual obligations). The data processor is only authorised to process the entrusted personal data in the scope and for the purposes set out in the agreement and may not use the data for its own purposes.

Since it is the data controller who maintains ultimate responsibility for data protection compliance, it is in his or her interest to appoint a reliable data processor. There is no obligation to carry out a service provider due diligence in the PDPA, nor is it required by the DPA. However, such approach is advisable before an agreement on entrusted data processing is concluded.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Under the PDPA, the transfer of personal data to third countries, (ie, outside of the EEA) is restricted. In general, such transfers are only permissible on the condition that the country of destination ensures an adequate level of personal data protection in its territory.

It should be added that, according to the PDPA, the adequacy of the level of personal data protection (referred to above) is evaluated taking into account all the circumstances concerning a data transfer operation, in particular the nature of the data, the purpose and duration of the proposed data processing operations, the country of origin and the country of final destination of the data as well as the legal provisions being in force in a given third country and the security measures and professional rules applied in this country.

However, there are certain circumstances in which a data transfer may be performed notwithstanding the above restrictions. Namely, those circumstances are:

- where the transfer of personal data results from an obligation imposed on the data controller by legal provisions or by the provisions of any ratified international agreement that guarantee adequate level of data protection;
- where the data subject has given his or her written consent;
- where the transfer is necessary for the performance of a contract between the data subject and the controller or takes place in response to the data subject's request;
- where the transfer is necessary for the performance of a contract concluded in the interests of the data subject between the controller and another subject;
- where the transfer is necessary or required by reasons of public interest or for the establishment of legal claims;
- where the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer relates to data that are publicly available.

32 Notification of cross-border transfer

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

In the event that none of the above situations applies, personal data may be transferred to a third country on the basis of a data transfer agreement (DTA) concluded between the data exporter and data importer. If the DTA is based on EU standard contractual clauses, it does not need to be approved by the DPA. The transfer may also be based, for example, on binding corporate rules, however, they still need the DPA's approval.

33 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 general, 'onward transfers' are only permissible on the condition that the further data recipient (importer) is also bound by principles that guarantee an adequate level of data protection. It is the data exporter's responsibility to ensure this.

Rights of individuals

34 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.

Every individual has control over the processing of his or her personal data contained in filing systems, and in particular this covers the right, among others, to:

- obtain extensive information on whether such a filing system exists and to establish the controller's identity, the address of its seat and its full name, and, in case the controller is a natural person, to obtain his or her address and his or her full name;
- obtain information as to the purpose, scope, and the means of processing of the data contained in the system;
- find out when his or her personal data began to be processed and details of the content of the data; and
- obtain information as to the source of his or her personal data, unless the controller is obliged to keep it confidential as a state, trade or professional secrecy, etc.

There is, however, a limit to the right of access: the data subject may exercise this to obtain information once every six months.

35 Other rights

Do individuals have other substantive rights?

Individuals whose data are being processed, are entitled not only to obtain information but also to:

(i) demand the data to be completed, updated, rectified, temporarily or permanently suspended or erased, in case they are not complete, outdated, untrue or collected with violation of the PDPA, or in case they are no longer required for the purpose for which they have been collected;

(ii) make a justified demand in writing, for the blocking of the processing of his or her data, due to his or her particular situation – in cases where the processing of the data is necessary for the performance of tasks provided for by law and carried out in the public interest or the processing of the data is necessary for the purpose of the legitimate

interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject;

(iii) object to the processing of his or her personal data, should the controller intend to process the data for marketing purposes or object to the transfer of the data to another controller – in cases where the processing of the data is necessary for the performance of tasks provided for by law and carried out in the public interest or the processing of the data is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject; and

(iv) make a demand to a controller for reconsidering the data subject's individual case settled in contravention of article 26a paragraph 1 PDPA (according to which it is inadmissible for a final decision in an individual case of the data subject is to be issued solely based on automated processing of personal data in a computer system).

However, in cases referred to in points (ii) and (iv), if the data controller does not agree with the data subject's demand, he or she may refer the demand and the reasoning behind it to the DPA, who shall issue an appropriate decision.

Also, in the case referred to in point (iii), the data controller is allowed to leave the forename or forenames and the surname of the data subject in his or her filing system, along with his or her PESEL identification number or address – solely in order to avoid the data being used once more for the purposes to which the data subject objected.

36 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 file a civil law suit if they suffer damages due to a breach of personal data protection legislation. The data subject may claim that his or her 'personal interests' (as defined in the Polish Civil Code) have been injured or, if applicable, may also prove that he or she suffered a substantial loss. However, the payment of damages does not follow automatically – the affected individual needs to go through standard civil court procedure.

37 Enforcement

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

The above rights are exercisable either personally towards the data controller or through the judicial system (if the data subject suffered damages). In cases where the data subject feels that the data controller is acting in contravention of the personal data protection legislation, he or she may file a complaint to the DPA; however, this does not automatically lead to the payment of any damages. Nevertheless, on the basis of such a complaint, the DPA may issue an administrative decision that will force the data controller to act in accordance with the DPA's orders included in the decision.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

No.

Supervision

39 Judicial review

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

When a decision of the supervisory authority is issued data owners may, in the first instance, file a motion to the supervisory authority to reinvestigate the case. If the authority's decision is to keep the previous decision binding, then a data owner can appeal to the Voivodeship Administrative Court. A data owner can file an appeal from a verdict of the Voivodeship Administrative Court to the High Administrative Court.

Specific data processing

40 Internet use

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

A regime of storing information (cookies), in the terminal equipment of subscribers (end users) is provided by the TL.

The TL introduces the opt-in regime based on consent that can be expressed also by the use of software settings of specific equipment. The wording of article 173 (1) TL is as follows:

> *The storing of information or the gaining of access to information already stored in the telecommunications terminal equipment of a subscriber or a user is only allowed on condition that:*
> 1) *the subscriber or the end user is directly informed in advance in an unambiguous, simple and understandable manner with regard to:*
> a) *the purpose of storing and the manner of gaining access to this information,*
> b) *the possibility to define the conditions of the storing or the gaining of access to this information by using settings of the software installed on his telecommunications terminal equipment or a service configuration;*
> 2) *the subscriber or end user, having obtained information referred to in point 1), gives its consent;*
> 3) *the stored information or the gaining of access to this information do not cause changes in the configuration of the subscriber's or end user's telecommunications terminal equipment and in the software installed on this equipment.*

Article 173(2) TL states that 'the subscriber or end-user may give his consent (...) using the settings of the software installed on his telecommunications terminal equipment or a service configuration.' Thus, the TL Act provides for two models of expressing consent by subscribers (end users). The first classic model would be understood as explicit consent (not implied by any declarations of will of a different content). The second model, which derives from point 66 of the preamble to Directive 2009/136EC, is a non-standard model where consent is expressed by using software settings or a service configuration.

41 Electronic communications marketing

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

Currently a distinction must be made between electronic communications marketing and telecommunication marketing.

According to article 172 of the TL, the use of telecommunications terminal equipment and automated calling systems for the purposes of direct marketing shall not be allowed, unless the end user or subscriber has given his or her prior consent.

The amended article 172 of the TL has its origins in article 13 of the Directive 2002/58/EC. This applies mostly to natural persons and article 13 protects them against unsolicited communications. However, according to article 13, clause 5 of the above Directive: 'Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected'.

Subscribers and end-users, as defined in the TL, may be either natural or legal persons. Thus, article 172 of the TL protects both legal and natural persons who use communication devices, from unsolicited communications. In conclusion, under the TL, communication for direct marketing purposes is only allowed after receiving the end user's prior consent, whether it is a legal or natural person.

According to articles 209 and 210, whoever fails to obtain the end user's consent for direct marketing communications, as stipulated in article 172 of the TL, shall face a monetary fine that may reach up to 3 per cent of that entity's turnover from the last calendar year. Additionally, a fine of up to 300 per cent of the monthly salary may be imposed on the entity's officers in charge, in particular – members of the management board.

According to the ESSA, sending unsolicited commercial information specifically addressed to a natural person by electronic communications means, in particular via electronic mail, is prohibited. Commercial information shall be considered solicited, if the recipient has expressed his or her consent to receive such information. In particular, if he or she has made

available for the purpose of such receipt an electronic address that identifies him or her. The ESSA punishment for sending unsolicited mails is 5,000 zlotys. Additionally, the above-mentioned activity shall be regarded as unfair competition practice within the meaning of provisions of the Act of 16 April 1993 on Fighting Unfair Competition.

42 Cloud services

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

Currently in Poland there are no statutory regulations specifically with regard to cloud computing. It should be mentioned, however, that outsourcing personal data to the cloud constitutes entrusting data for processing within the meaning of the PDPA, therefore the provisions of article 31 of that act and underlying regulations (eg, as regards security measures) apply. Moreover, processing personal data in the cloud may require the transfer of data to non-EEA countries, which is also subject to special rules under the PDPA.

A piece of non-binding (although generally applied) regulation that touches upon the subject of cloud computing was issued in the scope of the banking sector – namely: Recommendation D (2013) of the Polish Financial Supervision Authority. The Recommendation lists general security measures that should be applied with regard to the use of cloud computing services by banks.

There are also obligations applicable to cloud computing stipulated in the Polish Telecommunications Law. Those regulations pertain to the obligation of securing data that is subject to telecommunications secrecy ('confidentiality of telecommunications' as referred to in the Telecommunications Law) and data retention requirements.

WIERZBOWSKI EVERSHEDS

Arwid Mednis **arwid.mednis@eversheds.pl**
Gerard Karp **gerard.karp@eversheds.pl**

Centrum Jasna
Ul. Jasna 14/16A
00-041 Warsaw
Poland

Tel: +48 22 50 50 700
Fax: +48 22 50 50 701
www.eversheds.pl

Russia

Ksenia Andreeva, Anastasia Dergacheva, 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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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 EC Data Protection Directive, but the Russian regulation places special emphasis on the technical (IT) measures for data protection. 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 (see 'Update and trends').

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 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.

According to the law currently in effect, administrative cases relating to violations of data privacy discovered by Roskomnadzor may be initiated by the prosecutor's office based on Roskomnadzor's administrative violations report. The administrative case is further considered by the court, which then makes an administrative ruling. According to the suggested amendments to the PD Law, Roskomnadzor could be entitled to initiate administrative cases without referring to the prosecutors' office, provided, however, that the imposition of administrative penalties is still the prerogative of a court.

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 issues related to personal data and the procedures for their 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'. Roskomnadzor also deals with requests and applications from individuals (see question 23).

Another important authority is the FSTEK. The 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. The FSTEK is often 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 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 the current Code for Administrative Offences of the Russian Federation, a data operator (and, as the case may be, its officers and other relevant employees) may be liable for a number of administrative offences in the data privacy sphere, including for violation of procedures for the gathering, storage, use or promulgation of personal data (article 13.11 of the Administrative Code), or failure to file or late filing to a government agency of necessary information on data processing activities (article 19.7 of the Administrative Code). Administrative liability for the offences is a fine of up to 10,000 roubles. In addition, the court may order the confiscation of uncertified information systems, databases and software used for data processing. In December 2014, the Russian parliament suggested strengthening the penalties for non-compliance with the PD Law (up to 300,000 roubles per violation).

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 such information 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.

Scope

4 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, classified information (ie, 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 (see the recommendations published on the website of the National Association of Non-Governmental Pension Funds at www.napf.ru/14154), for telecom operators (published on the website of the Ministry of Communications at www.minsvyaz.ru/uploaded/files/persdan.pdf), banks (published on the website of the Central Bank of the Russian Federation at www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf) and healthcare organisations (published on the website of the Ministry of Healthcare at: www.rosminzdrav.ru/documents/7570-rekomendatsii-ot-24-dekabrya-2009-g).

5 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 4).

6 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 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.

7 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.

8 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. Under Roskomnadzor's interpretation, published on its website, the PD Law applies to any legal entity, including any foreign entity with a legal presence in Russia, which collects personal data in Russia (see publication at http://pd.rkn.gov.ru/faq/faq17.htm).

In July 2014, the Russian State Duma approved amendments to the PD Law to include 'local storage requirements', which came into force on 1 September 2015 (Local Storage Law). In accordance with the new requirements, an operator is required to ensure that the recording, systemisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data is to be conducted only in 'databases located within Russia.' There are a number of exceptions to this requirement. For example, 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 within the foreign databases.

The Local Storage Law contains rather vague language, and there is still no official interpretation or other reliable guidance from Russian authorities on how to implement the new requirement. One of the most sensitive issues is whether the Local Storage Law applies to companies that have no legal presence in Russia but work with Russian individuals. While this remains unclear, it can be argued that companies with no corporate presence in Russia (either in the form of a subsidiary, a branch or a representative office) should not be covered by the Local Storage Law. At the same time, online businesses with no local presence could still be affected, particularly if they customise their websites for Russian users or promote their services in Russia.

9 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?

The PD Law does not distinguish between 'data controllers' and 'data processors'. Instead, a company engaged in data processing is a 'data operator' that organises or carries out (alone or with other operators) the processing of personal data and a company or individual who determines the purpose, content and method of personal data processing is a 'data operator'.

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 29). 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

10 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 are 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 are 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 are 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 are 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 have 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.

11 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 include an individual's full name, passport details, profession and education, and in essence amount to any personal data other than sensitive or biometric data;
(ii) sensitive data, which include 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

12 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.

13 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 the 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 were 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 were made publicly available by the individual or were received from a publicly available source;
- the personal data are 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.

14 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.

If such consent was not required or was implied, the individual would be able to control the use of his or her information only upon obtaining access to the data by a request to the data operator (see question 34). In cases where the data processed by the operator are inaccurate or irrelevant for the purpose of processing, the individual may request that the data operator rectify, block or delete his or her personal data and may raise an objection against the purpose or method of processing with Roskomnadzor or in court.

15 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).

16 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.

17 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 are 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.

18 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

19 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, the 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 the FSTEC. 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 the FSTEC or the FSS.

20 Notification of data breach

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

Article 21 of the PD Law provides for obligations related to data security breaches. These include an obligation on the data operator to rectify any breach (including a security breach) within three days and to notify the affected individual within three days of rectification. In the event of a rectification made at Roskomnadzor's request, the data operator must inform Roskomnadzor within three days of rectification. In practice, however, the notification requirement for security breaches rarely appears to be implemented or enforced.

Internal controls

21 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, but arguably, this should be the case. The officer must report directly to the general manager (director) and is responsible for the 'internal application of the provisions of the PD Law' 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.

22 Record keeping

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

The PD Law requires the data operator to establish a system of internal (local) documents with a detailed description of protective measures taken by the operator ('organisational measures' of protection). One of the protective measures required from the data operator to secure the data 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 only granted for a temporary period and for business needs.

Registration and notification

23 Registration

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

Yes, data operators are registered with Roskomnadzor in the following way.

The data operator must notify Roskomnadzor before starting to process personal data. This is a one-off notification and the data operator does not need to notify the authority in each instance of data processing. The data operator should amend the notification if the information contained in the initial notification changes. Roskomnadzor maintains a public register of data operators, based on the information contained in the notifications received. In the absence of any queries, Roskomnadzor acknowledges receipt of the notification and adds the information on the data operator to the register within 30 days of receipt of notification.

Most collection and processing of data requires formal notification to Roskomnadzor. There are exceptions for simple, one-off collections of data and HR-related data. For example, exemptions apply if:

- the data are processed under employment law only;
- the data are received by the data operator in connection with a contract with the individual, provided that such personal data are 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;
- the data relate to a certain type of processing by a public association or religious organisation;
- the data were made publicly available by the individual;
- the data consist only of the surname, first name and patronymic of the individual; or
- the data are necessary for granting one-time access to the individual into the premises where the data operator is located and in certain other cases.

24 Formalities

What are the formalities for registration?

The notification form can be found on Roskomnadzor's website at www.pd.rkn.gov.ru, together with guidance on its completion. The notification must contain:

- 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 operator's IT systems and security measures, 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.

25 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 Code for Administrative Offences of the Russian Federation. The same administrative penalties are imposed for late submission of the notification or amendments thereto.

26 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.

27 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 at http://pd.rkn.gov.ru/operators-registry/operators-list; 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.

28 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.

Transfer and disclosure of PII

29 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 10).

30 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. If such consent is obtained by the data operator, there are no restrictions on the disclosure to which consent was given. The recipient of the personal data must maintain the security and confidentiality of such data under the agreement with the data operator.

Update and trends

Russia continues to follow the European route and tightens the regulation of PD processing. In particular, Roskomnadzor has recently proposed to expand the regulations of PD Law so that it also covers all 'individual's data', with the definition of the latter to be developed. In addition, the regulator has recently stated that laws governing 'big data' must be created.

However, other issues of information processing are currently at the forefront of lawmaking activity (eg, regulation of those who disseminate information on the internet). Further development of the current draft initiatives and clarification of the recently adopted amendments is anticipated in the near future. It remains to be seen how the new approaches to the regulation of PD, such as the Local Storage Law, evolve in practice.

31 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 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. 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.

32 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.

33 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

34 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 are 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 are 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 are 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.

35 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 are inaccurate, unlawfully obtained or unnecessary for the purpose of processing by the data operator.

36 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.

37 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

38 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

39 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.

Morgan Lewis

Ksenia Andreeva **ksenia.andreeva@morganlewis.com**
Anastasia Dergacheva **anastasia.dergacheva@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

Specific data processing

40 Internet use

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

Russian law does not regulate the use of 'cookies'. There is also no official guidance on this subject by Roskomnadzor.

41 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).

42 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.

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The Personal Data Protection Act 2008 (DP Act), governs the collection and use of PII. Serbia has not fully implemented Directive 95/46/EC on data protection. However, the DP Act is consistent with some of the basic principles of the Data Protection Directive.

Sectoral laws also apply to PII processing in particular areas (see questions 5 and 6).

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 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

4 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.

5 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.

6 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 Records Act 1998 on collecting and keeping the PII in the healthcare sector;
- High Education Act 2005 on PII processing within the sector of high education;

- Education System Act 2009 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.

7 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)'.

8 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.

9 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?

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

10 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).

11 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

12 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.

13 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.

14 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 33 and 34).

15 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.

16 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.

17 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.

18 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

19 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 eight years since the implementation of the law, the government has not adopted such an act.

20 Notification of data breach

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

The law does not require PII owners to notify the Commissioner and the affected individuals of the data breach. The Commissioner has not issued any guidance in relation to this matter.

Internal controls

21 Data protection officer

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

Appointment of a data protection officer is not mandatory.

22 Record keeping

Are owners 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.

Registration and notification

23 Registration

Are PII owners and/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.

24 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 22 (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.

25 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.

26 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 due 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.

27 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 information contained in the filing system, if this is necessary for the

achievement of a prevailing interest of national or public safety, national defence, performance of the tasks by the 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.

28 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.

Transfer and disclosure of PII

29 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.

30 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.

31 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.

32 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 (or draft 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 usually takes a few months.

33 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. The PII owner who applies for the initial transfer should include in the request, as an important aspect of the transfer, a reference to onward transfers, if any, to the PII processors or PII users. There has been no conclusive practice from which one might infer whether the Commissioner's decision on permissibility of the initial transfer depends on the Commissioner stance vis-à-vis the permissibility of the secondary transfer.

Rights of individuals

34 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.

35 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 the PII individuals 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 circumstance 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.

36 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).

37 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

38 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

39 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

40 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.

41 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.

42 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 **bivanisevic@bdklegal.com**
Milica Basta **mbasta@bdklegal.com**

Majke Jevrosime 23
Belgrade 11000
Serbia

Tel: +381 11 3284 212
Fax: +381 11 3284 213
www.bdklegal.com

Singapore

Lim Chong Kin and Charmian Aw
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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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; 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); and
- Advisory Guidelines on Enforcement of Data Protection Provisions (Enforcement Guidelines).

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; and
- Guide to Disposal of Personal Data on Physical Medium.

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.

While Singapore has not formally adopted international instruments on privacy or data protection, 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 Flow of Personal Data and the APEC Privacy Framework, in developing the PDPA framework.

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 established as a statutory body under the PDPA on 2 January 2013 and is under the purview of the Ministry of Communications and Information (the MCI). The members of the PDPC are appointed by the MCI and the PDPC is currently chaired by Mr Leong Keng Thai, who is also the Deputy Chief Executive Officer of the Infocomm Development Authority of Singapore (IDA). Under him are four other members, namely:

- Ms Aileen Chia, Assistant Chief Executive and Director-General (Telecoms and Post), the IDA;
- Mr Ong Tong San, Cluster Director (Competition and Resilience Development), the IDA;

- Mr Yeong Zee Kin, Assistant Chief Executive, the PDPC; and
- Ms Ong Seok Leng, Senior Director (Governance Group), the IDA.

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 the 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 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 34 and 35 respectively for more information on access and correction requests).

The PDPA also establishes the Data Protection Advisory Committee, which advises the PDPC on matters relating to the review and administration of the personal data protection framework, such as key policy and enforcement issues. Currently, the Advisory Committee comprises 12 members and is headed by Ms Liew Woon Yin, director of Abundanti and former director-general of the Intellectual Property Office of Singapore. Of the 12 members, six new members from the banking, healthcare, IT, public, social services sectors and academia, were appointed on 28 January 2015 to contribute perspectives from each sector to the Advisory Committee.

3 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 February 2016 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 February 2016, 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 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 has voluntarily offered a remedy to the individual, and that individual has accepted the remedy;
- the organisation taking immediate steps to reduce the damage caused by a breach (such as informing individuals of steps they can take to mitigate risk); and
- the organisation voluntarily disclosing 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 36 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 to 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. Refer to question 25 for more circumstances under which criminal sanctions may be imposed under the PDPA.

Scope

4 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 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).

5 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 10 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, 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 34 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 IDA), 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 service-based operation licences may have to comply with interception requests by the IDA and other authorities. Specifically, condition 16 of the IDA's standard SBO (I) licence conditions expressly permit disclosure of subscriber information 'where disclosure of subscriber information is deemed necessary by [the] IDA or such other relevant law enforcement or security agencies in order to carry out their respective functions or duties'. Condition 26.1 of the IDA's standard SBO (I) licence conditions also require licensees to 'provide [the] IDA with any document and information within its knowledge, custody or control, which [the] IDA may, by notice or direction require'.
- Section 15A of the Computer Misuse and Cybersecurity Act 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'.
- Section 20 of the Criminal Procedure Code empowers the police to require the production of a 'document or other thing' (that 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 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'.

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 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.

6 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 deals with computer system hackers and other similar forms of unauthorised access or modification to computer systems;
- the Electronic Transactions Act 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 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 contains provisions that prohibit any disclosure of information relating to remuneration, payroll tax and income tax;
- the Private Hospitals and Medical Clinics Act 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 contains provisions relating to the prevention of disclosure of official documents and information;
- the Statutory Bodies and Government Companies (Protection of Secrecy) Act details provisions concerning protecting the secrecy of information of statutory bodies and government companies; and
- the Telecom Competition Code issued under the Telecommunications Act contains certain provisions pertaining to the safeguarding of end-user service information. Notably, the IDA 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 2012 – Amendments to AML/CFT Notices, which set out its proposed amendments to the MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism (AML/CFT). 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 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 market intermediaries;
- financial advisers;
- life insurers;
- holders of money-changer's licences and remittance licences;
- 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 their personal data that is in the possession or under the control of the FI.

7 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.

8 Extraterritoriality

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

Data protection provisions

No, 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.

9 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?

Yes, the PDPA regulates the collection, use and disclosure of personal data by organisations. All organisations that collect, use or disclose personal data are accordingly required to comply with the data protection provisions under the PDPA.

'Data intermediaries', however, are exempt from the majority of the data protection provisions under the PDPA. These refer to organisations that process personal data on behalf of and for the purposes of another organisation (the principal organisation) pursuant to a written contract. Data intermediaries are only required to comply with the rules relating to the protection and retention of personal data (see question 29 for further details), while the principal organisation is subject to the full suite of data protection provisions under the PDPA as if it was processing the personal data itself.

Legitimate processing of PII

10 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 from 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 Schedule 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.

11 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 19).

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 are also excluded from most of the obligations under the PDPA. In relation to such data, organisations will only be subject 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

12 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 10). In particular, organisations are obliged to inform individuals of:

(i) the purposes for the collection, use and 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 and 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 and 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 personal data collected is to be used for a different purpose than 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.

13 Exemption from notification

When is notice not required?

Generally, the obligation to notify the individual does not apply in situations where the collection, use or disclosure of personal data is authorised under any other written law, or where the individual's consent is deemed to have been given.

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 (refer to question 10 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.

14 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 an individual who has withdrawn his or her consent to the same.

15 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 personal data that 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 personal data that it collects (whether directly from the individual concerned or through another organisation);
- 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).

16 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.

17 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.

18 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 than those for which the individual concerned had given his or her consent (see question 10).

Security

19 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.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and 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, 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 avoid 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:

- extent of the data breach;
- type and volume of personal data involved;
- cause or suspected cause of the breach;
- whether the breach has been rectified;
- 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 3).

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

21 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 of these obligations) under the PDPA.

The public guidance published on the PDPC's website as of May 2016 sets out that the possible responsibilities of a DPO may include, but are not limited to, the following:

- developing good policies for handling personal data that are in compliance with the PDPA and are suitable to the organisation's needs;
- communicating internal data protection policies and processes to employees and customers;
- handling personal data related queries or complaints;
- alerting the organisation to any risks that might arise with regard to personal data; and
- liaising with the PDPC on data protection matters, if necessary.

22 Record keeping

Are owners 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 34), 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 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.

Registration and notification

23 Registration

Are PII owners and/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 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 telemarketing calls or send telemarketing messages (collectively referred to as specified messages) are required to, within 30 days before sending such messages, check the relevant DNC registers to ensure that recipient telephone numbers have not been registered before sending such specified messages.

24 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 in any one of three methods:

- by calling a toll-free number to access the automated Interactive Voice Responsive 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.

25 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.

26 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.

27 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 to, within 30 days before sending such messages, 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 will receive 1,000 free credits every year (up from 500 free credits previously), which will be 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.

28 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.

Transfer and disclosure of PII

29 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 only subject 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.

30 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 10 and 12).

Furthermore, in certain circumstances the PDPA restricts an organisation from providing an individual with:

- his or her personal data; 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 such individual has requested access to such personal data or information pursuant to the PDPA. See question 34 for a list of circumstances under which an individual's right to access his or her personal data is restricted.

31 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;
  - 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.

32 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.

33 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 31). 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 9 and 29 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 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 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 onwards 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 onwards transfers of personal data are conducted in accordance with the requirements of the PDPA.

Rights of individuals

34 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, which 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 the 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 provides 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;
- 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
- the prohibition under section 21(3)(c) of the PDPA does not apply where the other individual has consented to the disclosure of his personal data, or where any of the exceptions listed under the Fourth Schedule of the PDPA may apply.

The Key Concepts Guidelines further provides that 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.

35 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

Update and trends

On 11 July 2016, the Singapore government introduced the Info-communications Media Development Authority Bill in Parliament. The Bill provides for the formation of a converged infocommunications and media regulator, namely the Info-communications Media Development Authority (IMDA), and is expected to be passed in Parliament towards the later part of 2016. The IMDA will be formed through a merger of the current infocommunications and media regulators, namely the Info-communications Development Authority of Singapore and Media Development Authority of Singapore respectively. As part of this reorganisation, the existing PDPC, which is the statutory body responsible for administering the PDPA, will be dissolved. In its place, the IMDA will be designated as the new PDPC responsible for administering the PDPA.

2016 has been an active year in the area of data protection enforcement. On 21 April 2016, the PDPC issued its first batch of enforcement decisions against 11 organisations for breaches of data protection obligations under the PDPA. Five organisations were issued remedial directions (four of which included financial penalties), while six others were issued warnings. More recently, the PDPC has issued further enforcement decisions against other organisations in June and July of 2016.

In April 2016, the Singapore government announced that it intends to introduce a new Cybersecurity Bill, to be tabled in Parliament in 2017, as part of its review into the policy and legislative framework for cybersecurity. If enacted by Parliament, the new Cybersecurity Act is expected to confer additional powers on the Cyber Security Agency to manage cybersecurity incidents and raise the standards of cybersecurity providers. It is also intended to ensure that operators take steps to secure critical information infrastructure and report cybersecurity incidents. More substantive details of the new legislation are expected to be released in due course.

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 36).

36 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 has become 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.

37 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 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 of 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

38 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;
  - 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; and
- 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.

Supervision

39 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

40 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 and 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 makes 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.

41 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 27 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 5.

42 Cloud services

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

Generally, cloud computing service providers (CCSPs) are statutorily required to comply with the PDPA (in particular, the obligation to implement reasonable security arrangements to protect personal data in its possession or under its 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

DREW & NAPIER

Lim Chong Kin **chongkin.lim@drewnapier.com**
Charmian Aw **charmian.aw@drewnapier.com**

10 Collyer Quay
10th Floor, Ocean Financial Centre
049315 Singapore

Tel: +65 6531 4110
Fax: +65 6535 4864
www.drewnapier.com

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 that 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 IT Standard 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 IDA 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.

Slovakia

Radoslava Rybanová and Jana Bezeková
Černejová & Hrbek, sro

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The fundamental law concerning PII in the Slovak Republic is the Personal Data Protection Act No. 122/2013 as amended (PDPA). The PDPA implements provisions of the European Directive 95/46/EC.

In addition, the right to privacy is guaranteed by the Slovak Constitution. The Civil Code contains protection of personality rights including an individual's right to privacy.

Specific laws and regulations govern data collection and data processing for specific areas, operators or data subjects, such as the Labour Code provisions concerning employees' privacy; the Electronic Communications Act governing the use of telephone, facsimile and email data; and the Banking Act provides for banking secrecy rules with respect to the data of banking customers, etc. There are also a number of laws enabling or permitting personal data processing for various purposes, such as statistics, health care and social security, etc.

In addition, the Slovak Republic is bound by international treaties concerning data protection, such as the European Convention on Human Rights and Fundamental Freedoms. As a member country of the OECD, Slovakia also follows the OECD guidelines.

2 Data protection authority

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

The Slovak data protection authority is the Data Protection Office of the Slovak Republic (the Office). The Office is an independent state authority, established and governed by the PDPA.

The Office has the authority to:

- monitor and supervise the processing of personal data that relates to individuals;
- accept notifications concerning any suspicion of breach of the PDPA;
- investigate any suspicion of a breach of the PDPA, in particular to perform the inspection of data processing and to summon the data owner or data agent;
- impose measures for rectification in order to remove the detected deficiencies; and
- impose penalties for breaches of the PDPA.

3 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 PDPA may lead to the Office imposing rectification measures or penalties.

If such a breach also constitutes a breach of privacy rights protected under the Civil Code, it may also lead to an individual pursuing a private claim.

A breach of the PDPA may lead to criminal sanctions if the breach is serious and constitutes an offence pursuant to the Criminal Code, namely when an individual unjustly handles (processes, transmits, publishes, etc) data of an individual or individuals obtained with respect to his or her public function or another occupation or position. Such an offence may be penalised with imprisonment for up to one year or up to two years in the case of serious consequences, or when the offence is committed publicly.

Scope

4 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 types of personal data processing by all operators.

That means that state agencies are also, technically, subject to the PDPA. However, there are a number of exemptions for state bodies and agencies from the general obligations imposed by the PDPA, including the necessity to obtain consent of the data subject or to provide him or her with a notice on processing.

Such exemption is given for specific processing purposes, such as state security (security services), state defence (army), public order and safety (police), criminal prosecution (police, courts, prosecutors), ethics-related surveillance in regulated professions (chambers and bars) and important economic or financial interests of the Slovak Republic or EU, such as currency, fiscal and tax matters (tax and financial offices).

Another type of exemption is provided to specific organisations, irrespective of the purpose of processing: the National Security Office and the security services are exempt from the supervision of the Office with respect to data protection, and they may only be supervised by the National Council of the Slovak Republic (the Parliament).

5 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 also governs data processing for the purpose of marketing communication, monitoring and surveillance of individuals.

In addition, electronic marketing communication (eg, via email and telephone) is subject to the Electronic Communications Act.

Surveillance of employees in the workplace is governed by the Labour Code.

6 Other laws

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

As already mentioned, use of email, telephone and other similar data is subject to the Electronic Communications Act. Banks are also subject to the PDPA, but banking secrecy and data processing in banking operations are also governed by the Banking Act. Other credit institutions are governed

by the PDPA and they do not benefit from some exemptions given to the banks. Therefore there exists banking system credit information shared among banks and separate private credit information systems for non-banking creditors, the latter based solely on the consent of debtors for their credit data processing.

The PDPA enables data processing without the consent of the data subject, if such processing is determined in detail by a specific law (see question 10). As a result, there are a number of laws, which contain such data protection 'licences', including the laws on the various registries (eg, the property register), laws relating to health and social insurance, etc.

7 PII formats

What forms of PII are covered by the law?

The PDPA covers all types of PII, irrespective of the format, manner of collection or processing.

8 Extraterritoriality

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

The PDPA applies to data owners and data processors operating in the Slovak Republic and those operating abroad if they operate on territory where the Slovak Republic has jurisdiction. The PDPA also applies to data owners who operate in EU member states but whose means of automated data processing is located in the Slovak Republic.

9 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?

The PDPA applies to any processing or use of PII (such as collecting, storing, transferring and giving access).

There is a distinction made between the person who sets the purpose and means of the processing, namely the data owner and the person who provides services to data owners – the 'data agent'.

In general the data owner is responsible to the data subjects for the handling of data by data agents. He or she must make sure the data agent is bound by a written contract.

Legitimate processing of PII

10 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 processing (including its collection and holding) is permitted only on specific grounds determined by PDPA.

Processing of personal data is permitted if:

- the purpose of processing, group of data subjects and the list or scope of personal data are stipulated in a specific law or international treaty binding on the Slovak Republic;
- the data subject has given his or her consent; or
- one of the following specific legal grounds determined by the PDPA occurs:
  - PII is processed for the purposes of literal or artistic work, news and public information. In such cases, however, the privacy rules of the Civil Code must be followed;
  - processing is necessary for fulfilment of a contract, to which the data subject is a party, or during a precontractual relationship;
  - processing is necessary for the protection of life, health or property of the data subject;
  - the title, first name, surname and address of the data subject is processed solely for mailing purposes;
  - solely previously legitimately published data is processed;
  - processing is necessary for an important task in the public interest; or
  - processing is necessary for the protection of rights and legally protected interests of the data owner or a third party. Such processing includes property monitoring by security cameras or similar security systems. Such processing is not possible if it may infringe data subjects' protected rights, which in that specific case should prevail over the interests of the data owner or another third party. Data subjects may object to their PII processing on the basis of this ground.

11 Legitimate processing – types of PII

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

The PDPA defines 'specific categories of data' for which the PDPA determines more stringent rules.

These categories include sensitive data, namely those revealing race or ethnicity, political views, religion, political party membership, trade union membership, health or sex life of an individual. Processing of such sensitive data is in general prohibited, and it may be undertaken only in exceptional cases determined by the PDPA, such as where:

- data are processed with the written or otherwise provable consent of the concerned individual;
- data are processed on the grounds of a specific law or international treaty binding for the Slovak Republic;
- processing is necessary for the protection of the vital interests of the data subject;
- data concerning the religion, political party or trade union membership are processed by the specific organisations (ie, church, political party, trade union) solely for internal purposes; and
- health data are processed by the healthcare providers.

Specific categories of data also include 'general identifier of an individual', processing of which is limited to strictly necessary purposes. This relates mainly to the 'birth number', which is a unique number identifying an individual attributed to each Slovak citizen at birth or to the resident foreigner in the residency permit, and is used in identification documents and state security and pension systems or health insurance systems.

The PDPA limits the processing of psychological profiles. This is permitted only to psychologists, or where such processing is expressly required under a specific law (with respect to the permit to own a gun or licences for professional drivers, etc).

Processing of criminal record data and information on administrative offences is only permitted if it is requested or permitted under a specific law.

Data handling responsibilities of owners of PII

12 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 PDPA requires data owners to provide extensive notification to the data subjects before or at the time of their personal data collection.

Such notice must contain:

- identification of the data owner and his or her representative (if any);
- identification of the data agent;
- the purpose of data processing;
- a list of processed personal data or their scope; and
- any other information that the data subject may need in order to use or apply for his or her rights, such as:
  - the identification of the person who will collect the data;
  - information on whether data provision is voluntary or mandatory;
  - if data are collected on the basis of a consent of data subject, information on the duration of such consent;
  - if data are collected on the basis of a specific law or international treaty, information on consequences of refusal to provide the data;
  - information about third parties to whom data will be provided or recipients to whom data will be made available;
  - if data are to be published, it must be stated in the notice together with the manner of publishing; and
  - any other countries to which data will be transferred, if that is the case.

The PDPA requests that data subjects be informed in detail of their rights ensuing from the PDPA.

If the data owner has received PII from another person (ie, he or she was its recipient and not original owner), he or she must provide the same notice to data subjects if their data are transferred or provided to any third parties.

If the data owner operates a video surveillance system, it is necessary to mark the monitored areas appropriately.

13 Exemption from notification

When is notice not required?

When data are processed on the grounds of a binding international treaty or under a specific law that expressly determines the list of personal data and purpose of its processing, notice is not required. However, if data are processed on the basis of a specific law, they may be provided or made available to the third party, transferred or published only if that is expressly permitted by such law together with the list of permitted recipients or a manner of publishing.

Notice is also not required if data are processed for the purposes of creation of literary or artistic work or news and public information, provided that privacy protection rules of the Civil Code are followed.

If data are processed for the purposes of historic or scientific research or statistics, notice is not required if it would be objectively impossible or require unreasonable efforts.

Notice is also not required when only previously published data is processed.

Data owners who did not collect personal data themselves have a general obligation to give notice to the data subjects before they provide or transfer their data to the third party; however, such notice is not required if they can prove that data subjects have already been duly notified.

14 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 owner must inform data subjects whose data are collected in detail about their rights under the PDPA. Such rights include not only access to data but also the possibility to ask for correction, blocking or discarding of data under the conditions determined by the PDPA. If data are processed on the basis of the consent, the PDPA gives the possibility of the data subject withdrawing consent, even before expiration of its term.

15 Data accuracy

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

The PDPA stipulates that only true, correct, complete and current data may be processed. The data owner is responsible for data being correct, complete and current. Whoever provided data to the system is responsible for data being true.

Whenever the data owner learns that data are not correct or complete, he or she is obliged to block the data and correct and complete such data without delay. If that is not possible, the data owner is obliged to mark incorrect data and discard them without delay. Data subjects may also ask for their data to be corrected or discarded if incomplete or incorrect data is processed.

16 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?

Only such data may be collected and processed that are required for the purpose of processing.

As for duration of processing, the law prescribes that PII must be destroyed as soon as the purpose of their processing has expired or has been fulfilled. The exemption is granted only to data contained in the written reports or documents that must be archived for a certain time. According to the law, those must be destroyed after said time has expired.

17 Finality principle

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

The PDPA implements the finality principle according to which data may be only used for the purpose for which they were collected. It is not permitted to merge data collected for various purposes.

18 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 general, it is not possible to introduce a new purpose for processing previously collected data. An exemption is given to the purposes of historical or scientific research and statistics. If possible, data should be anonymised for such new uses and destroyed as soon as such purpose has been fulfilled.

Security

19 Security obligations

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

The data owner is obliged to protect the personal data against damage, destruction, loss, change, unauthorised access or dissemination, provision or unauthorised publishing. For such purposes, the data owner is obliged to implement technical, organisational and personnel measures. Such measures must be adequate to the type of data and technical manner of their processing and therefore based on the thorough evaluation of risks by the data owner. The PDPA, however, does not specify detailed security measures.

In some cases specified by the PDPA, for example, when a data system is connected to the internet and contains sensitive data, the data owner must issue such security measures in a written document (called the 'security project') and must submit such project for inspection to the Office upon request. That may be the case for HR information systems, which may contain sensitive data (eg, health checks of employees).

The data processors have the same scope of security obligations under the law as the data owners. In addition, they should be bound by the written contract determining their obligations towards the data owner.

20 Notification of data breach

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

There is no express obligation in the PDPA to notify the Office or data subjects if a security breach or leak occurred. There is no specific guidance of the Office recommending breach notifications.

Internal controls

21 Data protection officer

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

Appointment of a data protection officer is not mandatory. However, if the data owner appoints a data officer, he or she is exempt from the obligation to notify the data systems to the Office.

The data protection officer must be a physical person fully capable of legal acts, must be trustworthy (have a clean criminal record) and must pass the exam set by the Office.

The data owner must give full access to all data systems containing PII to the data protection officer. The data protection officer must be able to independently supervise the protection of personal data.

The data protection officer is responsible for reviewing whether data processing infringes the rights and freedoms of data subjects. He or she is obliged to cooperate with the Office's monitoring activities. The data protection officer is also responsible for ensuring that all entitled persons (ie, persons who have access to the processed data) are given appropriate information on their duties according to the PDPA and internal rules (such as the confidentiality duty).

The data protection officer deals with the requests of the data subjects and ensures that they are complied with, implements security measures and supervises data transfers to the data processors or transborder transfers.

The data protection officer is responsible for maintaining the internal records of the data systems and is obliged to submit specific registration of such systems to the Office when registration of the system is prescribed by the PDPA.

22 Record keeping

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

Data owners are obliged to keep internal records on all systems, which are exempt from the notification obligation to the Office.

Internal records of the systems contain the same information that would otherwise be included in the notification to the Office (see question 23). Such internal records must be made available to anyone upon request free of charge.

Registration and notification

23 Registration

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

The data owner is obliged to notify the Office about all data systems, which at least partially use automated data processing, unless one of the following four exemptions applies:

- the data system is subject to the registration;
- the data owner appointed a data protection officer;
- the data system contains personal data of persons in a specific organisation (eg, trade union, church, political party), and if these personal data are processed and used solely for its internal needs; or
- the personal data are processed on the legal grounds determined by the law (either the PDPA or another specific law) or international treaty binding on the Slovak Republic.

The Office reviews whether the notification is complete, assigns a specific identification number to the system and sends confirmation to the data owner.

A registration duty applies on all data systems that contain:

- personal data processed without the consent of data subjects for the protection of the interests of a data owner or a third party, if the Office decides that registration is required;
- biometric data (except if provided otherwise by a specific law); and
- sensitive data designated for transfer to a third country without an adequate level of protection.

The data owner must send the registration form, including prescribed information, and pay the registration fee to the Office. The Office then evaluates whether the system triggers the risk of infringement of the rights and freedoms of data subjects. The Office may refuse to register the system when it sees such a risk (see question 26).

24 Formalities

What are the formalities for registration?

There is no fee payable for the notification of systems to the Office.

Notification must be given on the form issued by the Office and it must contain the identification data of the data owner, the number of persons having access to such a system, the name of the data system, purpose and legal grounds of data processing, scope of data subjects, list or extent of processed data, third parties to which data is provided or made accessible, the manner and legal grounds of publishing (if data is published) and the third countries to which data is transferred, if applicable. Notification must also, in a general way, determine the security measures used to protect data and state the intended start date of processing.

The registration fee is €50 per data system. The registration must be submitted on the registration form issued by the Office. The registration must contain the identification data of the data owner, the number of persons having access to it, the name of the system, purpose and legal grounds for data processing, scope of data subjects, list or extent of processed data, third parties to which data is provided or made accessible, manner and legal grounds of publishing of data, third countries to which data is transferred, if applicable, determination of security measures and the date of the start of processing. The registration application must also determine the reason for registration of the data system.

25 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 penalty for failure to submit the application for registration is a minimum of €1,000 rising to a maximum of €200,000.

The penalty for failure to submit the notification to the Office and for failure to maintain internal records is up to €3,000.

26 Refusal of registration

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

The Office may refuse to register the data system if there is a risk that data subjects' rights and freedoms will be infringed. Following such refusal, the data owner is obliged to take measures that will prevent the processing of personal data without undue delay.

For systems that are subject to notification, the Office may not refuse to confirm the notification, but may withhold it until complete information required by the PDPA is provided and notification is complete.

27 Public access

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

The register of data systems and list of notified data systems is publicly available. The Office shall allow access to these to anybody upon request.

The Office publishes information on the registered and notified systems on its website (www.dataprotection.gov.sk). Such information contains the identity of the data owner (name and identification number of the entity, or first name, surname and title of the physical person) and registration or identification number of the system.

28 Effect of registration

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

The data owner may start to process data in a system that is subject to the registration only after the registration of such a system by the Office. If the Office refuses to register the system, the data owner must remove and rectify all steps already done with respect to establishment of the system.

If the data system is subject to the notification, the data owner may start the processing from the date of notification.

Transfer and disclosure of PII

29 Transfer of PII

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

Outsourced processing of data (appointing of data agent) is only possible with a written contract executed between the data owner and such agent. The contract must contain identification of the parties, the start date of processing by an agent, the purpose of the processing, the name of the data system, a list or scope of processed data, group of data subjects, the conditions of processing including the permitted operations, the period for which the contract is valid, the date of execution and signatures of the parties.

The consent of a data subject is not necessary for transfer of data to the agent, provided that all conditions under the PDPA are observed.

30 Restrictions on disclosure

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

The PDPA distinguishes the disclosure (ie, making data accessible to the third party who does not further process them) and provision of data (ie, making data available to the third party for further processing); however, both are only permitted with the consent of the data subject and upon prior notice to the data subjects.

When data is processed without consent because their processing is based on a specific law, disclosure or provision of such data to the third party is only permitted when such law also specifies that they may be disclosed or provided and to whom.

Update and trends

Personal data protection legislation of the Slovak Republic, being a member state of the EU, will be vastly affected by the implementation of the new 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 and repealing Directive 95/46/EC (the Regulation) that shall apply from 25 May 2018. The Regulation overrides all national laws dealing with the same subject matter, hence the Slovak PDPA shall cease to be applicable in all matters governed by the Regulation, whether it will be definitions, obligations of the data owners, registration obligations, relationships with data processors and data transferees and indeed sanctions and penalties. Since the publication of the Regulation, the activities of the Office and the focus of data owners will be aimed at implementing and applying the new rules and obligations introduced by the Regulation. It is not likely therefore that any changes of the local PDPA or any substantial guidelines will be issued in 2017 or 2018.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The transfer of data to other EU member countries is not restricted; it is possible under the same conditions as transfer within the Slovak Republic. The data owner is, however, obliged to ensure the protection of rights and interests of data subjects during and after the transfer.

Transfers to third countries are divided into two regimes.

One regime applies to the transfer to the third countries providing an adequate level of data protection based on decisions of the European Commission. Transfer to such countries is not subject to any specific requirements.

Another more complicated regime applies to data transfers to third countries not providing an adequate level of data protection. Such transfer requires prior approval of the Office, unless:

- the data owner implemented adequate safeguards with respect to the protection of privacy and rights and freedoms of data subjects in the form of standard contractual clauses based on European Commission decisions or binding corporate rules approved by the data protection authority of one of the EU member countries;
- a data subject gave written consent with the knowledge that the country of final destination does not provide an adequate level of protection (informed consent); or
- such a transfer is necessary for the reasons specified in the PDPA (eg, performance of a contract with data subject, protection of the vital interests of data subject, important public interest).

Transfers to the US must follow the regime of the transfer to the third countries not providing an adequate level of protection, unless the conditions of the EU-US Privacy Shield are fulfilled. Transfers complying with the EU-US Privacy Shield scheme are treated as transfers to the country providing an adequate level of protection.

In any case, transfer of PII belonging to 'specific categories' (sensitive data) is possible only with the prior written consent of the data subject for such a transfer.

32 Notification of cross-border transfer

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

Approval of the Office is required for the transfer of personal data to the third countries not providing adequate level of data protection unless one of the conditions specified in question 31 is met. The Office shall commence a proceeding on granting approval for the transfer on the basis of a written application filed by the data owner. A period for issuing such approval is not determined by the law; in practice it usually takes several weeks.

33 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?

Transfers to service providers (agents) within the EU are possible upon the written contract executed between such an agent and data owner, without requiring any specific notification to, or consent of, the data subjects. For other transfers, the restrictions and limitations mentioned above fully apply.

Rights of individuals

34 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.

Concerned individuals have the right to access whether their data is processed as well as to receive a copy of such data. Individuals are also entitled to obtain further information, such as the source of data, purpose and means of processing, etc.

Exemptions are only given to the processing of data on the basis of specific laws, mainly by the state agencies, mentioned in question 4 (exempt sectors).

Individuals may exercise their right of access by the written request to the data owner or data processor (who is obliged to forward such request also to data owner). If the request is delivered by email, the written request must follow within three days (ie, email request alone is not sufficient). The request may also be recorded personally in the office of the data processor and the data processor is obliged to prepare the record of such a request, which should be dated and undersigned by the concerned individual.

The data owner has 30 days to comply with the delivered request of the concerned individual. The request should be complied with free of charge, except for the request for a list of the processed data when the data owner may charge actual costs of the technical data carrier and the mailing costs.

35 Other rights

Do individuals have other substantive rights?

Concerned individuals have the right to request correction or destruction of their incorrect, incomplete or outdated personal data or destruction of personal data, if the purpose for their processing has ended.

They also have the right to the destruction of their personal data in case of violation of the law.

If personal data is processed upon consent, data subjects may withdraw such consent even prior to expiration of the period for which it has been granted; in such case they may request the blocking of data.

Data subjects may object to the processing of their personal data for direct marketing purposes without their consent and call for their destruction, in which case the data owner must discard that data and notify all third parties to whom he or she has provided such data to do the same.

Data subjects may object to the processing of their personal data without their consent for the purpose of protecting the legitimate interests of the data owner and claim that such processing infringes their individual rights.

Data subjects may also object to, and not make themselves subject to, decisions of data owners based solely on automated data processing.

36 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 PDPA does not provide grounds for monetary compensation to the data subjects.

Individuals may have such right under the Civil Code if their personality rights have been infringed. The Civil Code contains in article 11 and following, the complete protection of personality rights. According to this, private documents, pictures, sound or video records concerning an individual or his or her personal actions can be made or used only with the consent of such individual (except for the official use on the basis of the law). Consent is not necessary for their use for scientific, artistic or informational

purposes provided that it is not contrary to the justified interests of the data subject. Also, the name, dignity and privacy of an individual are protected from the unauthorised infringement.

The concerned individual may request that infringement of his or her personality rights is stopped and all consequences are removed, and he or she may claim adequate compensation. The court may attribute such compensation in money to cover 'immaterial harm', such as injury to feelings.

37 Enforcement

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

The rights provided by the Civil Code are enforceable through a private court claim filed by the concerned individual. If the concerned individual is not capable of legal acts, action can be made by or his or her legal representative. Heirs may place the claim for the deceased person.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

The PDPA does not apply to data processing by individuals for personal and domestic purposes (such as correspondence or contact lists) or to data obtained randomly that are not further processed or categorised. The PDPA also does not apply to data concerning legal entities.

The name, surname and address of an individual may be processed for the purpose of direct marketing communication even without the consent of such a person. However, if the person has objected to such use, the data owner must block the data and stop using them. He or she must also inform anybody else to whom this data has been provided of the data subject's objection.

Supervision

39 Judicial review

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

Yes, decisions of the Office are reviewable by the courts by administrative action.

Specific data processing

40 Internet use

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

The use of cookies and similar technologies for storing information, and accessing information stored, on a user's equipment (computer, mobile, etc) is regulated by section 55(3) of the Electronic Communications Act, which stipulates that anyone who stores or obtains access to information stored in the terminal equipment of a user is entitled to do so only if the user has given his or her consent on the basis of clear and comprehensive information on the purpose of processing; the use of a respective setting of the web browser or another computer program is deemed as a consent for this purpose. The obligation to obtain consent does not apply to the competent criminal authorities and other public authorities. This shall not prevent technical storage of or access to data, the sole purpose of which is to transmit or facilitate the transmission of messages through the network, or if it is strictly necessary for the information society service provider to provide an information society service explicitly requested by the user.

The above provision of the Electronic Communications Act represents a complete transposition of article 5(3) of the e-Privacy Directive 2009/136/EC into the national law.

41 Electronic communications marketing

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

According to the Electronic Communications Act, marketing via email, facsimile or telephone is subject to the prior consent of the recipient. Such consent must be provable. Given consent may be revoked at any time.

Exemption is given to the direct email marketing communication sent to the customer, who gave contact data to the seller in respect to purchasing similar goods or services. Each marketing email must contain the identity and address of the sender, to which the recipient may send a request to unsubscribe from marketing communication.

42 Cloud services

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

There are no specific rules or guidance on cloud computing services. The transfer of any personal data to the cloud computing provider is subject to the obligations relevant for the data transfers as described in questions 29–31. The legal relationship between the data owner and the cloud computing services provider will most frequently have the character of the relationship between the data owner and the data agent (data processor). In all such cases the rules and obligations applicable for data transfers to the data processor will apply for the transfer of personal data to the cloud services. As a general rule, the data owner is responsible for data processing and data security during their processing by the data agent. The transfer of biometrical data to the cloud is not recommended as the guidelines of the Office (Methodical Guidelines 6/2013) state that transfer of such data to cloud computing should be avoided. The written contract between the data owner and the cloud services provider as data agent must be executed, and it is crucial for the data owners to have clear and enforceable obligations of the cloud services provider agreed in such a contract.

ČERNEJOVÁ & HRBEK
Advokátska kancelária Law Firm

Radoslava Rybanová **rybanova@chplaw.sk**
Jana Bezeková **bezekova@chplaw.sk**

Kýčerského 7
81105 Bratislava
Slovakia

Tel: +421 2 5244 4019
Fax: +421 2 5244 2650
www.chplaw.sk

South Africa

Danie Strachan and André Visser

Adams & Adams

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

There is currently no dedicated data protection legislation in South Africa. The protection of PII is dealt with on a piecemeal basis by various pieces of legislation, including the Consumer Protection Act 2008 (CPA), the National Credit Act 2005 (NCA), the Promotion of Access to Information Act 2000 (PAIA), the Electronic Communications and Transactions Act 2002 (ECTA) and the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA).

A dedicated data protection law in the form of the Protection of Personal Information Act 2013 (POPI) has been promulgated by Parliament. However, the Act is not yet in force (except for a few limited sections dealing with the establishment of the Regulator and the provisions allowing for the drafting of the regulations). The discussion that follows will be with reference to the data protection system that will be put in place by POPI. Where POPI is discussed in relation to a specific topic, it means that current legislation does not adequately cover the same. It should be noted that even though POPI has been promulgated by Parliament, the regulations have not yet been drafted and will contain a substantial amount of detail not yet provided by POPI.

2 Data protection authority

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

The PAIA regulates the rights of individuals to access information and is overseen by the Human Rights Commission.

POPI establishes the office of the Information Regulator, which will be responsible for overseeing the protection of PII. The powers, duties and functions of the Regulator include:

- providing education, by promoting an understanding and acceptance of the conditions for lawful processing of personal information, by promoting the protection of personal information through educational programmes, by making public statements on matters affecting the protection of personal information, by providing advisory services for the exercise of rights of data subjects, and by providing advisory services to responsible parties or ministers on any matter relevant to the operation of POPI;
- monitoring and enforcing compliance with the Act by both private and public bodies, by undertaking research and monitoring of developments in the information processing and computer technology to ensure that such developments do not have adverse effects, by examining any proposed legislation that could have an effect on the protection of personal information, by reporting to Parliament on any matter affecting the protection, by conducting assessments of public or private bodies to ascertain that the personal information is processed lawfully;
- consulting with interested parties by inviting and receiving representations from members of the public on matters affecting the personal information of a data subject, by cooperating at a national and international level with other persons or bodies concerned with the protection of personal information, and being a mediator in disputes pertaining to the protection of the personal information;
- handling complaints by receiving and investigating the complaints, providing relevant feedback to complainants, gathering information that will assist in discharging the duties and carrying out the functions of the Regulator, and resolving disputes using dispute resolution mechanisms such as mediation and conciliation;
- conducting research and reporting to Parliament from time to time on the desirability of acceptance of international instruments relating to the protection of personal information and on any matter including legislative amendments;
- in terms of codes of conduct, issuing, amending and revoking codes of conduct, making guidelines to enable bodies to develop or apply codes of conduct and reconsidering determinations by adjudicators under approved codes of conduct;
- facilitating cross-border cooperation by participating in any initiative aimed at the enforcement of privacy laws; and
- generally doing anything necessary for the performance of any of the outlined functions, to exercise and perform such functions, powers and duties as are conferred by the Regulator in terms of the Act, requiring the disclosure of the data subject whose data has been compromised to exercise the powers conferred upon the Regulator in terms of POPI.

The Regulator may publish reports relating to the exercise of the Regulator's functions, if it is in the public interest.

3 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 RICA, ECTA, PAIA, NCA and CPA have limited provisions that relate indirectly to data protection and, in certain instances, the breach of those provisions could lead to administrative or criminal sanctions or both. POPI provides for criminal sanctions to be imposed on any person upon conviction of an offence listed in POPI.

Any person convicted of an offence under the terms of POPI is liable to a fine or to imprisonment (ranging from a period not exceeding 12 months to a period not exceeding 10 years) or to both a fine and imprisonment. Administrative penalties may also be imposed.

Scope

4 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?

POPI applies to the processing of personal information entered in a record by or for a responsible party by making use of automated or non-automated means, provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.

POPI does not apply to the processing of personal information during a personal or household activity, or information that has been de-identified to the extent that it cannot be reidentified, or on behalf of a public body

where it involves national security, including activities aimed at the identification of the financing of terrorist and related activities, defence or public safety to the extent that adequate safeguards have been established in legislation for the protection of such personal information, or by the Cabinet, its committees or the executive council of a province, or relating to the judicial functions of a court.

The provisions of POPI do not apply to the processing of personal information solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression. Where a responsible party who processes personal information for exclusively journalistic purposes is, by virtue of an office, employment or profession, subject to a code of ethics that provides safeguards for the protection of personal information, such code will apply to the processing concerned to the exclusion of POPI and any alleged interference with the protection of the personal information of a data subject that may arise as a result of such processing must be adjudicated as provided for in terms of that code.

The Regulator may grant an exemption to a responsible party to process personal information by notice in the Gazette irrespective of whether the information is in breach of a condition for the processing of such information, provided the Regulator is satisfied that the public interest in processing substantially outweighs any interference with the privacy of the data subject that could result from such processing or the processing involves a clear benefit to the data subject or a third party that substantially outweighs any interference with the privacy of the data subject or third party that could result from such processing.

Personal information processed for the purpose of discharging a relevant function is exempt to the extent to which the application of those provisions to the personal information would probably prejudice the proper discharge of that function. In this context, function refers to any function of a public body or any function conferred on any person under law that is performed to protect members of the public against financial loss due to the dishonesty and malpractice of persons concerned in the provision of banking, insurance, investment or other financial services or the management of bodies corporate; or the dishonesty, malpractice or other seriously improper conduct or incompetence of persons authorised to carry out a profession or any other activity.

5 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.

POPI contains some provisions regulating electronic marketing (see question 41). However, the interception of communications is specifically governed by the RICA, which prohibits the monitoring or interception of communications unless it takes place in accordance with the RICA's provisions.

6 Other laws

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

The CPA contains specific provisions relating to direct marketing and consumer privacy. The NCA regulates the privacy of credit information. The ECTA contains certain voluntary data protection provisions in the context of electronic communication. The right to privacy is also enshrined in section 14 of the Constitution of the Republic of South Africa 1996.

7 PII formats

What forms of PII are covered by the law?

POPI is applicable to the processing of all PII entered in a record, which includes any recorded information regardless of its form or medium. A record is defined as any recorded information regardless of its form or medium, including writing on any material; information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored, with a label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; book; map; plan; graph or drawing; or photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced, in the possession or under the control of a responsible party, irrespective of whether it was created by a responsible party and regardless of when it came into existence.

In terms of POPI's definition, PII means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. It includes various forms of personal information, including:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

8 Extraterritoriality

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

POPI applies where the responsible party is domiciled in the Republic or not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

9 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?

POPI distinguishes between a 'responsible party', which means a public or private body or any other person, which alone or in conjunction with others determines the purpose of and means for processing personal information, and the 'operator', which means a person who processes personal information for a responsible party in terms of a contractor mandate without coming under the direct authority of that party.

Legitimate processing of PII

10 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?

Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

Personal information may only be processed if:

- the data subject (or a competent person where the data subject is a child) consents to the processing; processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
- processing complies with an obligation imposed by law on the responsible party;
- processing protects a legitimate interest of the data subject;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

The responsible party bears the burden of proof for the data subject's or competent person's consent. The data subject or competent person may at any time withdraw his or her consent, provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information will not be affected.

Processing of information is not in breach of a condition if the Regulator grants an exemption or processing is for the purpose of discharging a relevant function (as discussed above).

11 Legitimate processing – types of PII

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

POPI regulates specific personal information, which relates to the religious or philosophical beliefs, race, ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject, or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

The Regulator may, upon application by a responsible party and by notice in the Gazette, authorise a responsible party to process special information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject, and may impose reasonable conditions for authorisation granted.

The prohibition on processing personal information concerning a data subject's religious or philosophical beliefs does not apply if the processing is carried out by spiritual or religious organisations or independent sections of those organisations if the information concerns data subjects belonging to such organisations or it is necessary to achieve their aims and principles or if it is carried out by institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles, or other institutions provided that the processing is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing.

The prohibition does not apply to the processing of personal information regarding the religion or philosophy of life of family members of data subjects if the association concerned maintains regular contact with those family members in connection with its aims and family members have not objected in writing to the processing. Personal information concerning a data subject's religious or philosophical beliefs, which is processed in accordance with the exceptions mentioned above, may not be supplied to third parties without the consent of the data subject.

The prohibition on processing personal information concerning a data subject's race or ethnic origin does not apply if the processing is carried out to identify data subjects and only when this is essential for that purpose and to comply with the laws and other measures designated to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

The prohibition on processing personal information concerning a data subject's trade union membership does not apply if the processing is by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the objectives of the trade union or trade union federation. Even so, no personal information may be supplied to third parties without the consent of the data subject.

The prohibition on processing personal information concerning a data subject's political persuasions does not apply to the processing by or for an institution founded on political principles of the personal information of its members or employees or other persons belonging to the institution if such processing is necessary to achieve the objectives or principles of the institution or a data subject if such processing is necessary for the purposes of forming a political party, participating in the activities of or engaging in the recruitment of members for or canvassing supporters or voters for a political party with the view to an election of the National Assembly, the provincial legislature, municipal elections or a referendum.

The prohibition on processing personal information concerning a data subject's health or sex life does not apply to:

- processing by medical professionals, healthcare institutions or facilities or social services (if such processing is necessary for the proper treatment and care of the data subject or for the administration of the institution or professional practice concerned);
- insurance companies, medical aid schemes, medical aid scheme administrators and managed healthcare organisations (if such processing is necessary for assessing risk to be insured if the data subject has not objected to the processing, for the performance of an insurance or medical aid agreement or for the enforcement of any contractual rights and obligations);
- schools (if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life);
- any public or private body (if such processing is necessary in connection with the implementation of prisons sentences or detention measures); or
- administrative bodies, pension funds, employers or institutions working for them (if such processing is necessary for the implementation of the provisions of laws, pension regulations or collective agreements that create rights dependent on the health or sex life of the data subject, or the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity).

The responsible party can only process such information subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject. The responsible party must treat the information as confidential unless the responsible party is required by law to communicate the information to other parties who are authorised to process such information. Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained unless a serious medical interest prevails or the processing is necessary for historical, statistical or research activity.

The prohibition on processing personal information concerning a data subject's criminal behaviour does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law. The processing of information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

A responsible party may not process personal information concerning a child. The prohibition on processing the personal information of children does not apply if processing is carried out with the prior consent of a competent person, or if it is necessary for the establishment, exercise or defence of a right or obligation in law, or it is necessary to comply with an obligation of international public law, or for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned or it appears to be impossible or would involve a disproportionate effort to ask for consent and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent or of personal information that has deliberately been made public by the child with the consent of a competent person. The Regulator will, upon application by a responsible party and by notice in the Gazette, authorise such responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.

Data handling responsibilities of owners of PII

12 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 subject has the right to be informed that the personal information about him or her is being collected or that his or her personal information has been accessed or acquired by an unauthorised person.

Steps must be taken to ensure that the data subject is aware of the purpose of the collection of his or her information.

If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of:

- the information being collected and, where the information is not collected from the data subject, the source from which it is collected;
- the name and address of the responsible party;

- the purpose for which the information is being collected;
- whether or not the supply of the information by that data subject is voluntary or mandatory;
- the consequences of a failure to provide information;
- any particular law authorising or requiring the collection of information;
- the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;
- any further information such as the recipient or category of recipients of information;
- the nature or category of the information;
- the existence of the right of access to and the right to rectify the information collected;
- the existence of the right to object to the processing of personal information; and
- the right to lodge a complaint to the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed to enable processing in respect of the data subject to be reasonable.

The steps referred to above must be taken if the personal information is collected directly from the data subject, before the information is collected and unless the data subject is already aware of the information referred to or in any other case, before the information is collected or as soon as is reasonably practicable after it has been collected.

A responsible party that has previously taken steps in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information remains the same.

13 Exemption from notification

When is notice not required?

It is not necessary for a responsible party to comply with the notification provision if:

- the data subject or a competent person (where the data subject is a child) has provided consent for the non-compliance;
- the non-compliance would not prejudice the legitimate interests of the data subject;
- non-compliance is necessary to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences, to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue or for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated or in the interests of national security;
- compliance would prejudice a lawful purpose of the collection; or where compliance is not reasonably practicable in the circumstances of the particular case; or
- the information will not be used in a form in which the data subject may be identified or be used for historical, statistical or research purposes.

14 Control of use

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

A data subject has the right to have his or her personal information processed in accordance with the conditions for the lawful processing of personal information, including the right to object, on reasonable grounds relating to his or her particular situation, to the processing of his or her personal information and to object to the processing of his or her personal information at any time for the purposes of direct marketing.

A responsible party may only process the personal information of a data subject who is a customer of the responsible party if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his or her electronic details at the time when the information was collected and on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

15 Data accuracy

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

A responsible party must take reasonably practicable steps to ensure that PII is complete, accurate, not misleading and updated where necessary. In doing so, the responsible party must have regard to the purpose for which personal information is collected or further processed.

Personal information must be collected directly from the data subject except:

- if the information is contained in or derived from a public record or has deliberately been made public by the data subject;
- if the data subject or competent person has consented to the collection of the information from another source;
- if collection of the information from another source would not prejudice a legitimate interest of the data subject;
- if collection of the information from another source is necessary to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
- in order to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue or for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
- in the interests of national security or to maintain legitimate interests of the responsible party or of a third party to whom the information is supplied; or
- where compliance would prejudice a lawful purpose of the collection or where compliance is not reasonably practicable in the circumstances of the particular case.

The responsible party must restrict processing of personal information if its accuracy is contested by the data subject for a period enabling the responsible party to verify the accuracy of the information, the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for the purposes of proof, or the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead, or if the data subject requests to transmit the personal data into another automated processing system.

Personal information may, with the exception of storage, only be processed for the purposes of proof, with the data subject's consent, with the consent of a competent person, for the protection of the rights of another natural or legal person, or if such processing is in the public interest.

Where processing of personal information is restricted, the responsible party must inform the data subject before uplifting the restriction on processing.

A data subject has the right to have his or her personal information processed in accordance with the conditions for the lawful processing of personal information, including the right to request, where necessary, the correction, destruction or deletion of his or her personal information.

A data subject may, in the prescribed manner, request a responsible party to correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully or request that the responsible party destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain.

Upon receipt of such a request, the responsible party must correct the information, destroy or delete the information, provide the data subject to his or her satisfaction with credible evidence in support of the information or, where agreement cannot be reached between the responsible party and the data subject and if the data subject so requests, take such steps as are reasonable in the circumstances to attach to the information in such a manner that it will always be read with the information, and an indication that a correction of the information has been requested but has not been made.

If the information has been changed according to the request by the data subject and the change has an effect on decisions taken or still to be taken, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of such steps. The responsible party must also inform a data subject who has made a request of the action taken as a result of the request.

16 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?

Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless retention of the record is required or authorised by law, or the responsible party reasonably requires the record for lawful purposes related to its functions or activities, retention of the record is required by a contract between the parties, or the data subject or a competent person has consented to the retention of the record.

Records of personal information may be retained for periods in excess of those contemplated for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

A responsible party that has used a record of personal information of a data subject to make a decision about the data subject must retain the record for such period as may be required or prescribed by law or a code of conduct, or if there is no law or code of conduct prescribing a retention period, retain the record for a period, which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

A responsible party must destroy or delete a record of personal information or de-identify it as soon as is reasonably practicable after the responsible party is no longer authorised to retain such record.

The deletion or destruction of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

17 Finality principle

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

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

Steps must be taken to ensure that the data subject is aware of the purpose of the collection of the information.

18 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 of personal information must be in accordance with the purpose for which it was collected. To assess whether the further processing is compatible with the purpose of collection, the responsible party must take account of the relationship between the purpose of the intended further processing and the purpose for which the information has been collected, the nature of the information concerned, the consequences of the intended further processing for the data subject, the manner in which the information has been collected, and any contractual rights and obligations between the parties.

The further processing of personal information is not incompatible with the purpose of collection:

- if the data subject or a competent person has consented to the further processing of the information or where the information is available in or derived from a public record or has deliberately been made public by the data subject;
- where further processing is necessary to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
- in order to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue, or for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated or in the interests of national security;
- where the further processing of information is necessary to prevent or mitigate a serious and imminent threat to public health or public safety or the life or health of the data subject or another individual;
- where the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
- where the further processing of the information is in accordance with an exemption granted by the Regulator.

Security

19 Security obligations

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

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent the loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information.

The responsible party must take reasonable measures:

- to identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- must ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

A responsible party must have due regard to generally accepted information security practices and procedures that may apply to it generally or be required in terms of specific industry or professional rules and regulations.

An operator or anyone processing personal information on behalf of a responsible party or an operator must process such information only with the knowledge or authorisation of the responsible party, and treat personal information that comes to their knowledge as confidential and must not disclose it unless required by law or in the course of the proper performance of their duties.

A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator that processes personal information for the responsible party establishes and maintains the security measures as identified.

20 Notification of data breach

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

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Regulator and the data subject, unless the identity of such data subject cannot be established. The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system. The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification to a data subject must be in writing and communicated in at least one of the following ways: mailed to the data subject's last known physical or postal address, sent by email to the data subject's last known email address, placed in a prominent position on the website of the responsible party, published in the news media or as may be directed by the Regulator.

The notification of data must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the breach, including a description of the possible consequences of the breach, a description of the measures that the responsible party intends to take or has taken to address the breach, a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the breach and, if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

The regulator may direct a responsible party to publicise in any manner specified the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

Internal controls

21 Data protection officer

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

Each public and private body must make provision, in the manner prescribed in the PAIA, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the said duties and responsibilities and any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body.

An information officer's responsibilities include the encouragement of compliance by the body with the conditions for the lawful processing of personal information, dealing with requests made to the body pursuant to the Act, working with the Regulator in relation to investigations conducted pursuant to the Act and otherwise ensuring compliance by the body with the provisions of the Act or as may be prescribed. Officers must take up their duties in terms of this Act only after they have been registered with the Regulator by the responsible party.

22 Record keeping

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

A responsible party must maintain the documentation of all processing operations under its responsibility.

Registration and notification

23 Registration

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

This aspect is not addressed by POPI.

24 Formalities

What are the formalities for registration?

This aspect is not addressed by POPI.

25 Penalties

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

This aspect is not addressed by POPI.

26 Refusal of registration

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

This aspect is not addressed by POPI.

27 Public access

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

This aspect is not addressed by POPI.

28 Effect of registration

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

This aspect is not addressed by POPI.

Transfer and disclosure of PII

29 Transfer of PII

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

A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator that processes personal information for the responsible party establishes and maintains the security measures as identified.

The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

30 Restrictions on disclosure

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

There are no specific restrictions on the disclosure of PII to other recipients, but specific restrictions are imposed on the providers of processing services, as set out in question 29.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

A responsible party in South Africa may not transfer personal information about a data subject to a third party who is in a foreign country unless the third-party recipient is subject to a law, binding corporate rules, a binding agreement or a memorandum of understanding entered into between two or more public bodies that provide an adequate level of protection that effectively upholds principles for the reasonable processing of the information that is substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person, and includes provisions that are substantially similar to this section, relates to the further transfer of personal information from the recipient to third parties who are in a foreign country, the data subject consents to the transfer, the transfer is necessary for the performance of a contract between the data subject and the responsible party or for the implementation of precontractual measures taken in response to 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 responsible party and a third party, or the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer, and if it were reasonably practicable to obtain such content, the data subject would be likely to give it.

32 Notification of cross-border transfer

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

The responsible party must obtain prior authorisation from the Regulator prior to any transfer of special personal information or personal information of children to a third party in a country that does not provide adequate protection for the processing thereof.

33 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?

A responsible party in South Africa may not transfer personal information about a data subject to a third party who is in a foreign country unless the third party who is the recipient of the information is subject to a law, binding corporate rules, a binding agreement or a memorandum of understanding entered into between two or more public bodies, which provide an adequate level of protection that effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and where applicable a juristic person and includes provisions that are substantially similar to this section, relates to the further transfer of personal information from the recipient to third parties who are in a foreign country, the data subject consents to the transfer, the transfer is necessary for the performance of a contract between the data subject and the responsible party or for the implementation of precontractual measures taken in response to 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 responsible party and a third party, or the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer, and if it were reasonably practicable to obtain such content, the data subject would be likely to give it.

Update and trends

South Africa's data protection statute was published in final form a while ago, but there has been a delay in bringing the law into effect. However, there has been some movement recently, with the nomination of the members of the Information Regulator, but it is not yet clear when the legislation will enter into force.

Rights of individuals

34 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.

Having provided adequate proof, a data subject has the right to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject and request from such responsible party the record or a description of the personal information about the data subject held by the responsible party including information about the identity of all third parties or categories of third parties who have or have had, access to the information within a reasonable time, at a prescribed fee, in a reasonable manner and format and in a form that is generally understandable.

A data subject must be advised of the right to request the correction of information. Where the data subject is required by the responsible party to pay a fee for services provided, to enable the responsible party to respond, the responsible party must give the applicant a written estimate of the fee before providing the services and may require the applicant to pay a deposit for all or part of the fee. A responsible party may or must refuse to disclose any information requested to which the grounds for refusal of access to records as set out in the PAIA apply. If a request for information is made to a responsible party and part of such information may or must be refused, every other part must be disclosed.

The provisions of PAIA pertaining to the form of requests apply to requests made in terms of access to personal information.

A data subject has a right to have his or her personal information processed in accordance with the conditions for the lawful processing of personal information, including a right to establish whether a responsible party holds personal information of that data subject and to request access to his or her personal information.

35 Other rights

Do individuals have other substantive rights?

A data subject may, in the prescribed manner, request a responsible party to correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or request that the responsible party destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain.

Upon receipt of such a request, the responsible party must correct the information, destroy or delete the information, provide the data subject (to his or her satisfaction) with credible evidence in support of the information or, where agreement cannot be reached between the responsible party and the data subject and if the data subject so requests, take such steps as are reasonable in the circumstances to attach to the information an indication that a correction of the information has been requested but has not been made.

If the information has been changed according to the request by the data subject and the change has an effect on decisions taken or still to be taken, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of such steps. The responsible party must also inform a data subject who has made a request of the action taken as a result of the request.

A data subject has a right to have his or her personal information processed in accordance with the conditions for the lawful processing of personal information, including a right to request, where necessary, the correction, destruction or deletion of his or her personal information as provided for by POPI.

36 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?

A data subject or, at the request of the data subject, the Regulator may institute a civil action for damages against a responsible party for breach of any provision of the Act, regardless of whether there is intent or negligence on the part of the responsible party.

In the event of a breach, the responsible party may raise any of the following defences against an action for damages:

- force majeure;
- consent of the plaintiff;
- fault on the part of the plaintiff;
- compliance was not reasonably practicable in the circumstances;
- the Regulator has granted an exemption; or
- the breach was perpetrated by a recipient of personal information while they were a party to a non-binding memorandum of understanding between two or more public bodies.

A court hearing such proceedings may award an amount that is just and equitable, including the payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of the breach, aggravated damages in a sum as determined by the court, interest, and costs of the suit on such scale as may be determined by the court. Any amount awarded by the Regulator must be dealt with in the following manner: the full amount must be deposited into a specifically designated trust account established by the Regulator with an appropriate financial institution, the Regulator may recover all reasonable expenses incurred in bringing proceedings as a first charge against such amount, and if there is any balance remaining, the Regulator must distribute it to the data subject at whose request the proceedings were brought.

A court issuing an order must order it to be published in the Gazette and by such other appropriate public media announcement as the court considers appropriate. Any civil action instituted may be withdrawn, abandoned or compromised but any agreement or compromise must be made an order of court. If a civil action has not been instituted, any agreement or settlement may, on an application to the court by the Regulator after due notice to the other party, be made an order of court and must be published in the Gazette and by such other public media announcement as the court considers appropriate.

37 Enforcement

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

Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject. A responsible party or a data subject may submit a complaint to the Regulator in the prescribed manner and form if he or she is aggrieved by the determination of an adjudicator.

Upon receiving a complaint, the Regulator may:

- conduct a pre-investigation;
- act at any time during the investigation and where appropriate as conciliator in relation to any interference with the protection of the personal information of a data subject in the prescribed manner;
- decide to take no action on the complaint or require no further action in respect of the complaint;
- conduct a full investigation of the complaint; or
- refer the complaint to the Enforcement Committee or take such further action as is contemplated by the provisions of the Act.

If a responsible party is alleged to have committed an offence under the Act, the Regulator may deliver an infringement notice by hand to that person (hereafter referred to as the infringer), which must contain the following particulars:

- the name and address of the infringer;
- the particulars of the alleged offence; and
- the amount of the administrative fine payable, which may not exceed 10 million rand.

The Regulator must also inform the infringer that, not later than 30 days after the date of service of the infringement notice, the infringer may pay

the administrative fine or make arrangements with the Regulator to pay in instalments, or elect to be tried in court on a charge of having committed the alleged offence. The notice must state that a failure to comply with the requirements of the notice within the time permitted will result in the administrative file becoming recoverable by the Regulator, and a filing with the clerk of court or registrar for a liquid debt in the amount specified in the statement.

If an infringer elects to be tried in court for a charge of having committed the alleged offence under POPI, the Regulator must hand the matter over to the South African Police Service and inform the infringer accordingly.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

The Regulator may grant an exemption to a responsible party to process personal information by notice in the Gazette irrespective of the information being in breach of a condition for the processing of such information, provided the Regulator is satisfied that the public interest in the processing substantially outweighs any interference with the privacy of the data subject that could result from such processing or the processing involves a clear benefit to the data subject or a third party that substantially outweighs any interference with the privacy of the data subject or third party that could result from such processing.

Public interest could refer to:

- the interest of national security;
- the prevention, detection and prosecution of offences;
- important economic and financial interests of public bodies;
- fostering compliance with established legal provisions;
- historical, statistical or research activity; or
- the special importance of the interest in freedom of expression.

The Regulator may impose reasonable conditions in respect of any exemption granted.

Supervision

39 Judicial review

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

A responsible party on whom an information or enforcement notice has been served may, within 30 days of receiving the notice, appeal to the High Court having jurisdiction for the setting aside or variation of the notice. A complainant who has been informed of the result of the investigation by the Regulator may, within 180 days of receiving the result, appeal to the High Court having jurisdiction against the result.

Specific data processing

40 Internet use

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

This aspect is not directly addressed by POPI.

41 Electronic communications marketing

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

The CPA regulates direct marketing. Section 11 of the CPA provides consumers with the right to restrict unwanted direct marketing. This right includes the right to refuse, to accept, to require another person to discontinue or to pre-emptively block any direct marketing communication. A consumer may thus require any person who approaches the consumer for the purposes of direct marketing, within a reasonable time, to desist from initiating any further communication. The section also makes provision for the establishment of a registry in which consumers may register a pre-emptive block either generally or for specific purposes. The registry for pre-emptive blocking purposes is currently being established and the provisions relating to pre-emptive blocking are not yet in force. Consumers may rescind transactions that arise from direct marketing within a specified time period.

The ECTA also deals with unsolicited commercial communications. In terms of section 45 of ECTA, the sender must provide the recipient with the option to stop subscription to a mailing list. At the recipient's request, the sender must also provide the recipient with identifying particulars of the source.

POPI contains the following provisions relating to direct marketing:

- a data subject has a right not to have his or her personal information processed for direct marketing purposes by means of unsolicited electronic communications;
- a data subject has a right to have his or her personal information processed in accordance with the conditions for the lawful processing of personal information, including a right not to be subject, under certain circumstances, to a decision that is based solely on the basis of the automated processing of his or her personal information intended to provide a profile of such person as provided for in POPI;
- a data subject may at any time object to the processing of personal information in a prescribed manner, on reasonable grounds relating to his or her particular situation, unless legislation provides for such processing or for the purposes of direct marketing other than direct marketing by means of unsolicited electronic communications;
- the processing of personal information of a data subject for the purposes of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMS or email is prohibited unless the data subject has given his or her consent to the processing or is a customer of the responsible party;
- a responsible party may approach a data subject whose consent is required and who has not previously withheld such consent only once in order to request the consent of that data subject, in a prescribed manner and form;

Adams & Adams

Danie Strachan **danie.strachan@adamsadams.com**
André Visser **andre.visser@adamsadams.com**

Lynnwood Bridge, 4 Daventry Street
Lynnwood Manor
Pretoria 0081
South Africa

Tel: +27 12 432 6000
Fax: +27 21 432 6599
www.adamsadams.com

- a responsible party may only process the personal information of a data subject who is a customer of the responsible party if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service, for the purpose of direct marketing of the responsible party's own similar products or services, and if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his or her electronic details at the time when the information was collected and on occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use;
- any communication for the purpose of direct marketing must contain details of the identity of the sender or the person on whose behalf the communication has been sent and an address or other contact details to which the recipient may send a request that such communications cease; and
- a data subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through a directory inquiry service, in which his or her personal information is included, must be informed, free of charge and before the information is included in the directory, about the purpose of the directory and about any further uses to which the directory may possibly be put based on search functions embedded in electronic versions of the directory. A data subject must be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his or her personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use. These provisions are not applicable to directories produced in printed offline electronic form prior to the commencement of this section. If the personal information of data subjects who are subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in compliance with the conditions for the lawful processing of personal information prior to the commencement of this section, the personal information of such subscribers may remain included in this public directory in its printed or electronic versions, after having received the information required.

42 Cloud services

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

No rules or guidance has been issued.

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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 is the Data Protection Act (1998:204), which implements Directive 95/46/EC. The Data Protection Act (DPA) authorises the government and the data protection authority, the Swedish Data Inspection Board, to issue more detailed regulations concerning several important features of the Act. This authorisation has been relied on to issue the Data Protection Ordinance (1998:1191) and several Regulations published in the Data Inspection Board Statute Book (DIFS).

Swedish law uses the term 'personal data'. Personal data is defined by the DPA as 'all kinds of information that directly or indirectly may be referable to a natural person who is alive'. This chapter will use the term personal data rather than PII.

An estimated 200 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. Of relevant legislation outside of the Registry Acts may be mentioned the Camera Surveillance Act (2013:460) and the Electronic Communications Act (2003:389), implementing the ePrivacy Directive 2002/58/EC. 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.

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 its letter of instruction: 'to detect and prevent threats to personal privacy. Its activities shall prioritise areas considered particularly sensitive from a privacy perspective, new phenomena and applications of technology and where the risk of abuse or misuse is deemed to be particularly large'.

The DIB is a public authority reporting to the Ministry of Justice. It is a comparatively small organisation, comprising 56 employees in 2015 (45 full-time positions) with an operating budget for 2016 of approximately 48.7 million kronor. 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 2013 (2013:460).

The DIB's Annual Report for 2015 relates that the DIB initiated 53 new and finalised 87 ongoing inspection matters during 2015. The DIB's Annual Report for 2015 has ceased to break down whether these procedures were conducted as field inspections, inspections by written procedure or inspections by survey.

The DIB has the power to request access to such personal data that are 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 them.

3 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 DIB may, in connection with carrying out its investigative powers, 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 them. The DIB can also sanction its decisions through an administrative fine. If the DIB finds that a decision thus sanctioned has been breached, it cannot on its own authority enforce the administrative fine but has to seek a court order that the fine be paid. It is rare for the DIB to seek such enforcement and it has not occurred during 2015.

A person who intentionally or recklessly breaches certain specific sections of the DPA may be sentenced to imprisonment of at most six months or, if the offence is grave, to imprisonment of at most two years. A sentence shall not be imposed in petty cases.

The following breaches may constitute a criminal offence:

- failure to, where required, register and maintain an accurate entry in the register;
- failure to comply with a mandatory enforcement or information notice under the DPA or within the specified time;
- obstructing execution of a warrant of entry or failing to cooperate or providing false information;
- wrongful processing of sensitive personal data; and
- wrongful transferring of personal data to a third country.

Only the Prosecution Authority can prosecute criminal offences under the DPA. Prosecution may be brought on the Prosecution Authority's own initiative or following a complaint from the DIB, from a perceived victim or from the general public. During the period 2006 to 2010 only two criminal cases were prosecuted under the DPA, out of some 400 complaints.

Scope

4 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 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 have precedence over 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.

Following an amendment to the DPA in 2007, personal data that are not part of or are not intended to be part of a collection of personal data structured in a fashion to significantly facilitate the search or ordering of personal data (termed 'unstructured material') are exempt from most of the provisions of the DPA. The exemption, however, does not apply if processing of unstructured material entails an infringement of the data subject's privacy.

5 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 (2013:460) regulates the use of equipment for audiovisual 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.

6 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.

7 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 are included in or are intended to form part of a structured collection of personal data that are available for searching or compilation according to specific criteria, such as an indexed collection of paper documents.

8 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 who are established in Sweden. It is also applicable when the controller is established in a third country but for the processing of the personal data uses equipment that is situated in Sweden. However, this does not apply if the equipment is only used to transfer information between a third country and another such country.

9 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?

Processing is defined in the DPA as any operation or set of operations that is taken as regards personal data regardless of whether it occurs by automatic means, for example collection, recording, organisation, storage, adaptation or alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction.

The DPA distinguishes between data controller and 'personal data assistants' as well as those persons who work under the assistant's or the controller of personal data's direction. The term personal data assistant corresponds with the term 'processors' in the Data Protection Directive.

Legitimate processing of PII

10 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 DPA, personal data may be processed only if the data subject has given his or her consent to the processing or, if the processing is necessary in order:

- to enable the performance of a contract with the data subject or to enable measures that the data subject has requested to be taken before a contract is entered into;
- that the controller of personal data should be able to comply with a legal obligation;
- that the vital interests of the data subject should be protected;
- that a work task of public interest should be performed;
- that the controller of personal data or a third party to whom the personal data are provided should be able to perform a work task in conjunction with the exercise of official authority; or
- that a purpose that concerns a legitimate interest of the controller of personal data or of such a third party to whom personal data are provided should be able to be satisfied, if this interest is of greater weight than the interest of the data subject in protection against violation of personal integrity.

11 Legitimate processing – types of PII

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

The DPA makes a distinction for sensitive personal data. Sensitive personal data are PII that reveal:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs; or
- membership of a trade union and personal data as concerns health or sex life.

The processing of such personal data is prohibited unless the data subject has given his or her explicit consent, or that the data subject has made the information public in a clear manner.

Sensitive personal data may also be processed if the processing is necessary in order that:

(i) the controller of personal data should be able to comply with his or her duties or exercise his or her rights within employment law;
(ii) the vital interests of the data subject or some other person should be able to be protected and the data subject cannot provide his or her consent; or
(iii) legal claims should be able to be established, exercised or defended.

Information that is processed on the basis of (i) may be disclosed to a third party only if there is an obligation within employment law for the controller to do so or if the data subject has explicitly consented to the disclosure.

Non-profit organisations with political, philosophical, religious or trade union objectives may within the framework of their operations process sensitive personal data concerning the members of the organisation and such other persons who by reason of the objectives of the organisation have regular contact with it. However, sensitive personal data may be provided to a third party only if the data subject explicitly consents to it.

Sensitive personal data may be processed for health and hospital care purposes, provided the processing is necessary for:

- preventive medicine and healthcare;
- medical diagnosis;
- healthcare or treatment; or
- management of health and hospital care services.

A person who operates as a professional within the healthcare sector and who is subject to a duty of confidentiality may also process sensitive personal data that is subject to the duty of confidentiality. This also applies to the person who is subject to a similar duty of confidentiality and who has received sensitive personal data from the operation within the healthcare sector.

Sensitive personal data may be processed for research purposes, provided the processing has been approved in accordance with the Act (2003:460) on Ethics of Research on Humans.

Sensitive personal data may be processed for the purpose of statistics, provided there are legitimate grounds for processing and provided the interest of society in the statistics project within which the processing is included is manifestly greater than the risk of improper violation of the personal integrity of the individual that the processing may involve. Regarding statistical purposes, if the processing has been approved by a research ethics committee, the prerequisites are deemed satisfied. Research ethics committee means such special body for consideration of research ethics issues that has representatives for both the public and the research and that is linked to a university or a university college or to some other body that to a very substantial extent funds research.

Personal data may be disclosed for use in research and statistics projects unless otherwise is provided in the rules on secrecy and confidentiality.

Information about personal identity numbers or classification numbers may, in the absence of consent, only be dealt with when it is clearly justified having regard to:

- the purpose of the processing;
- the importance of a secure identification; or
- some other noteworthy reason.

Data handling responsibilities of owners of PII

12 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?

If data about a person is collected from the person himself or herself, the controller shall, in conjunction with collection, voluntarily provide the data subject with information about the processing of the data.

If personal data has been collected from a source other than the data subject, the controller shall provide the data subject with information about the processing of the data upon registration. However, if the data is intended to be disclosed to a third party, the information need not be given before the data has been disclosed for the first time.

13 Exemption from notification

When is notice not required?

Information need not be provided if there are provisions concerning the registration or disclosure of personal data in an Act or some other regulation. In addition, information does not need to be provided if it proves to be impossible or would involve a disproportionate effort. However, if the data is used to take measures concerning the data subject, the information shall be provided at the latest in conjunction with such measure taking place.

14 Control of use

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

A controller is liable at the request of the data subject to immediately rectify, block or erase such personal data that have not been processed in accordance with the DPA or regulations that have been made under the Act. The controller shall also notify a third party to whom the data have been disclosed about the measure, if the data subject requests it or if more substantial damage or inconvenience for the data subject could be avoided by a notification. However, no such notification need be provided if it is shown to be impossible or would involve a disproportionate effort.

A controller must provide the data subject with a copy of the personal data it holds on him or her upon request.

Personal data may not be processed for purposes concerning direct marketing, if the data subject gives notice in writing to the controller that he or she opposes such processing.

15 Data accuracy

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

A controller is obligated under the DPA to ensure that the personal data that are processed are correct and, if it is necessary, up to date, and that all reasonable measures are taken to correct, block or erase such personal data that are incorrect or incomplete having regard to the purposes of the processing.

16 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 DPA states that the controller shall ensure that no more personal data are processed than is necessary having regard to the purposes of the processing, and that personal data are not kept for a longer period than that as is necessary having regard to the purpose of the processing. The law does not provide an explicit time frame of permissible holding. In guidelines, the DIB has stated that personal data related to a business transaction should not be held longer than a year after the relation to the customer has expired.

Personal data may be kept for historical, statistical or scientific purposes for a longer time than necessary for the purpose for which they were collected. However, in such cases personal data may not be kept for a longer period than is necessary for these purposes.

17 Finality principle

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

The DPA states that the controller shall ensure that personal data are only collected for specific, explicitly stated and justified purposes, adopting the finality principle.

18 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 is 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.

Security

19 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, according to the DPA, implement appropriate technical and organisational measures to protect the personal data that is processed. The measures shall provide a level of security that is appropriate having regard to:

- the technical possibilities available;
- what it would cost to implement the measures;
- the special risks that exist with processing of personal data; and
- how sensitive the personal data processed really are.

If the controller engages a personal data assistant (a processor), the controller is required to ensure for himself or herself that the personal data assistant can implement the security measures that must be taken and to ensure that the personal data assistant actually takes the measures.

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.

20 Notification of data breach

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

There is no general notification requirement for data breaches in the DPA. The DIB does not demand that such notification is done on the basis of general good practice.

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 for 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 over 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 impact 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 is to be fulfilled. The Regulation came into force on 4 April 2016.

Internal controls

21 Data protection officer

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

It is not mandatory to appoint a data protection officer.

The DPA states the data protection officer's responsibilities as independently ensuring that the controller processes personal data in a lawful and correct manner and in accordance with good practice and also points out any inadequacies to him or her.

If the data protection officer has reason to suspect that the controller is in breach of the provisions applicable for processing personal data and if rectification is not implemented as soon as is practicable after being pointed out, the data protection officer should notify the DIB.

The data protection officer shall also otherwise consult with the DIB when uncertain of how the rules applicable to processing of personal data shall be applied.

The data protection officer shall maintain a register of the processing that the controller carries out and that would have been subject to notification if the representative had not been appointed. The register shall comprise at least the information that a notification would have contained.

The data protection officer shall assist data subjects to obtain rectification when there is reason to suspect that the personal data processed are incorrect or incomplete.

22 Record keeping

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

Yes, unless the controller has notified the DIB of such processing of personal data that it carries out. Maintaining an internal record of processing being performed can be an alternative to notification.

Registration and notification

23 Registration

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

Processing of personal data as such is subject to a general obligation to notify the DIB about the processing. There are several broad exemptions to this obligation and in practice notification is unusual in Sweden.

Registration is, for example, not required when:

- the personal data are being processed with the consent of the data subject;
- a data protection officer has been appointed;
- personal data are being processed in the context of 'unstructured material';
- personal data are processed by non-profit organisations with political, philosophical, religious or trade union objectives within the framework of their operations process where the data concerns the members of the organisation and such other persons who by reason of the objectives of the organisation have regular contact with the data;
- personal data are processed under a sector-wide agreement that has been reviewed by the DIB; or
- relating to certain types of personal data specified in the regulation DIFS 2013:1: where the controller maintains a record of the processing operation.

Processors are not subject to the registration requirement.

24 Formalities

What are the formalities for registration?

The registration with the DIB is done by submitting a notification form supplied by the DIB. There is no fee and the registration is valid indefinitely.

Notifications shall be made in writing and be signed by the data controller or its authorised representative. Notifications shall contain:

- the name, address, telephone number and corporate registration number of the data controller;
- the purpose or purposes of the processing operation;
- a description of the category or categories of data subjects affected by the data processing;
- a description of the category or categories of data concerning the data subjects that are to be processed;
- details of the recipients or categories of recipients to whom the data may be disclosed;
- information concerning any data transfer to third countries; and
- a general description of the measures that have been taken to safeguard the security of processing operations.

Any change in the above circumstances shall be notified in the same way.

25 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 intentionally or through recklessness fails to register a notification where required may be sentenced to imprisonment of at most six months or, if the offence is grave, to imprisonment of at most two years. A sentence shall not be imposed in petty cases.

Processors are not subject to the registration requirement.

26 Refusal of registration

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

The DIB may only refuse a registration if it is incomplete.

27 Public access

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

The DIB will answer questions about the content of the register but the register as an entity is not publicly available (eg, over the internet). Questions about the content of the registry can be submitted informally to the DIB by phone, email or other means suitable.

28 Effect of registration

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

No, not beyond fulfilling the statutory registration requirement.

Transfer and disclosure of PII

29 Transfer of PII

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

The DPA states that a personal data assistant (a processor) and a person or those persons who work under the assistant's or the controller of personal data's direction may only process personal data in accordance with instructions from the controller.

There must be a written contract on the processing by the personal data assistant of personal data on behalf of the controller of personal data. It shall be specifically stipulated in the contract that the personal data assistant may only process personal data in accordance with instructions from the controller and that the personal data assistant is liable to take appropriate technical and organisational measures to protect the personal data that is processed.

30 Restrictions on disclosure

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

Any disclosure of PII to other recipients must be covered by the general requirements of notice, choice and purpose limitation. No specific disclosure restrictions apply.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Transfer to a third country of personal data that are undergoing processing is prohibited unless the third country has an adequate level of protection for personal data. The provision also applies to transfer of personal data for processing in a third country. 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 the 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;
- 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 (BCR) have been implemented, if the BCR have been approved by the DIB.

It is also permitted to transfer personal data for use only in a state that has acceded to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The DIB has not, as of July 2016, made any comment regarding the EU commission's adoption of the Privacy Shield adequacy decision.

32 Notification of cross-border transfer

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

Not as such. The transfer in itself constitutes a processing of personal data, which requires notification unless an exemption applies as related above.

33 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 apply equally to transfers to service providers and onwards transfers.

Rights of individuals

34 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 controller of personal data is liable to provide once per annum, to every natural person who requests it, free-of-charge notification of whether personal data concerning the applicant are processed or not. If such data are processed, written information shall also be provided about:

- which information about the applicant is processed;
- where this information has been collected;
- the purpose of the processing; and
- to which recipients or categories of recipients the information is disclosed.

An application for information shall be made in writing to the controller and be signed by the applicant. The requested information shall be provided within one month from when the application was made. However, if there are special reasons for doing so, the information may be provided within four months from when the application was made.

Information does not need to be provided about personal data in running text that has not been given its final wording when the application was made or which comprises an aide memoire or similar. However, this does not apply if the data have been disclosed to a third party or if the data were only processed for historical, statistical or scientific purposes or, as regards running text that has not been given its final wording, if the data have 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 who 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.

35 Other rights

Do individuals have other substantive rights?

Individuals have the right to require rectification, blocking or erasing as applicable of such personal data that have not been processed in accordance with the DPA or regulations that have been made under the DPA. The controller must also notify a third party to whom the data have been disclosed about the measure, if the data subject requests it or if more substantial damage or inconvenience for the data subject could be avoided by a notification. However, no such notification need be provided if it is shown to be impossible or would involve a disproportionate effort.

The data subject is entitled to at any time revoke consent that has been given in those cases where the processing of personal data is only permitted on the basis of consent. Further personal data about the data subject may not subsequently be processed.

A data subject is not entitled, beyond where consent is a requirement or as concerns direct marketing, to object to such processing of personal data as is permitted under this DPA.

36 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.

Update and trends

The DIB became the supervisory authority for the Camera Surveillance Act (2013:460) on 1 July 2013. During 2015 the DIB has challenged in court 44 decisions where local county administrative boards had granted rights to conduct camera surveillance. Most of the challenges were ruled in favour of the DIB. These judgments from administrative courts elaborate the legal restrictions applying the use of surveillance equipment. A judgment from the Administrative Court of Appeal from December 2015 confirms that the Camera Surveillance Act applies to unmanned aircraft systems (also known as drones). The judgment has been appealed to the Supreme Administrative Court which has decided to take the case but not yet, as of July 2016, issued its ruling.

The DIB has, as the supervisory authority, investigated the authority in charge of welfare payments, Swedish Social Insurance Agency (SSIA), regarding its use of web cameras. SSIA had launched a service offering web meetings with a case officer. DIB found that such use of cameras was regulated by the Camera Surveillance Act. SSIA had also failed to seek union approval of the web camera usage. While DIB agreed that there was a legitimate reason for the camera usage, this did not outweigh the privacy concerns of the employee and the web camera usage as practised by SSIA was banned.

A security company, together with representatives from the petrol industry, developed a mechanism to combat the occurrence of people filling up their vehicles with petrol and then leaving without paying. The mechanism recorded details related to the non-payment (such as time and place, make of vehicle, registration number and outstanding payment) to an IT system. The system retrieved information on the vehicle's owner through public records and sent a notification to the owner of the non-payment. The mechanism also scanned the registration plates of cars at petrol stations prior to the pump being engaged. If the plate matched with a recording in the IT system of a non-payment, pre-payment was automatically imposed before the pump would function.

As only public authorities may process personal data regarding crimes, the parties seeking to deploy this mechanism applied to the DIB for an exemption. The DIB decided not to grant an exemption on the basis that while the proposed mechanism sought to preserve the opportunity of using petrol pumps prior to paying while preventing repeated fraud, this interest did not outweigh the privacy concerns connected with a centralised blacklist. The DIB decision was appealed up to the Supreme Administrative Court which upheld the DIB.

In preparation for the EU General Data Protection Regulation coming into force in May 2018, the Swedish government has tasked a number of official commissions to propose amending the existing legislation that would be impacted. The commissions will, inter alia, recommend levels of sanctions and possible changes to the scope of the DIB's responsibilities.

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 that his personal data had been 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 has appealed this latter award as too high.

37 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 may be enforced either through the court system, for example, through criminal prosecution, or by the DIB. In many cases, the DIB does not have the power to issue orders on its own authority, but must apply for a court order, for instance in order to have illegally processed personal data erased.

Exemptions, derogations and restrictions

38 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 limitation to the DPA is the subsidiarity rule that if another statute or other enactment contains provisions that deviate from the DPA, those provisions shall apply.

After an amendment to the DPA in 2007, personal data that are not part of or are not intended to be part of a collection of personal data structured in a fashion to significantly facilitate the search or ordering of personal data (termed 'unstructured material') are exempt from most of the provisions of the DPA. The exemption, however, does not apply if processing of unstructured material entails an infringement of the data subject's privacy.

Supervision

39 Judicial review

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

Yes, all orders by DIB may be appealed to the Stockholm Administrative Court.

Specific data processing

40 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, 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.

41 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.

42 Cloud services

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

The DPA applies to the use of cloud computing services as well – 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 offenses 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.

WESSLAU SÖDERQVIST

Henrik Nilsson **henrik.nilsson@wsa.se**

Kungsgatan 36, PO Box 7836
Stockholm 10398
Sweden

Tel: +46 8 407 88 00
Fax: +46 8 407 88 01
www.wsa.se

Switzerland

Lukas Morscher and Kaj Seidl-Nussbaumer
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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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 and its additional protocol of 8 November 2001.

Although Switzerland is not a member of the EU and, hence, has not implemented the EU Data Protection Directive 95/46/EC, it has been officially recognised by the European Commission as providing an adequate level of protection for data transfers from the EU.

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 23) or if there is a duty to provide information in connection with a cross-border data transfer (see question 32). 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.

3 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 10) 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.

Scope

4 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.

5 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 Intelligence Services (scheduled to enter into force in 2017);
- the Swiss Federal Unfair Competition Act;
- the Swiss Federal Code of Obligations; and
- Ordinance 3 to the Employment Act (regarding employee monitoring).

6 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;
- 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 scheduled to enter into force in 2017).

Further regulations may apply depending on the given subject matter.

7 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.

8 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).

9 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?

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 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

10 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 11) 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.

11 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 5 and 6.)

Data handling responsibilities of owners of PII

12 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.

13 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.

14 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 34 et seq.

15 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.

16 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.

17 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.

18 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 10).

Security

19 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.

20 Notification of data breach

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

There is no general data security breach notification obligation under Swiss data protection law. As a rule, it would contravene 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.

Internal controls

21 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.

22 Record keeping

Are owners 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 34), 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.

Registration and notification

23 Registration

Are PII owners and/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 due 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.

24 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.

25 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.

26 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.

27 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.

28 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.

Transfer and disclosure of PII

29 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 2008/7 relating to outsourcing issued by the FINMA applies to banks and securities dealers organised under Swiss law, including Swiss branches of foreign banks and securities dealers, which are subject to FINMA supervision. Before outsourcing a significant business area, these institutions must comply with the detailed measures set out in the circular, including:

- mandatory information of bank customers affected by the outsourcing;
- careful selection, instruction and control of the supplier; and
- conclusion of a written contract with the supplier setting out, among other things, the supplier's obligation to comply with professional secrecy rules.

30 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 10 and 11. 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 29 for requirements) does not constitute such disclosure.

Regularly disclosing information contained in a PII collection entails a registration obligation for such collections.

31 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/themen/00794/00827/index.html?lang=en). 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 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. Until Switzerland reaches a new agreement with the US, other safeguards such as data transfer agreements or binding corporate rules need to be implemented in order to lawfully transfer personal data from Switzerland to the US. Judging from past experience, any new agreement will likely be based on the US–EU Privacy Shield but would have to take into account particularities of Swiss data protection laws such as the protection of personal data of legal entities. No plan of action or timeline of any sort has been communicated by Swiss authorities yet.

32 Notification of cross-border transfer

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

As stated in question 31, 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.

33 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 (like, eg, the FDPIC's model data transfer agreement does).

Rights of individuals

34 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.

35 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.

Update and trends

The Swiss Federal Council has announced a revision of the DPA. The respective draft for an updated DPA is expected to be published by the end of August 2016 and is supposed to take into account the General Data Protection Regulation of the EU as well as the pending revision of the Convention of the European Council for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, and to strengthen the enforcement of individuals' rights and the protection of minors.

Regarding the US-Swiss Safe Harbor Framework, refer to question 31.

36 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.

37 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

38 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

39 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

40 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.

41 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.

42 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 19). 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 29 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 31 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/datenschutz/00626/00876/01203/index.html?lang=en).

LENZ & STAEHELIN

Lukas Morscher **lukas.morscher@lenzstaehelin.com**
Kaj Seidl-Nussbaumer **kaj.seidl-nussbaumer@lenzstaehelin.com**

Bleicherweg 58
8027 Zurich
Switzerland

Tel: +41 58 450 80 00
Fax: +41 58 450 80 01
www.lenzstaehelin.com

Taiwan

Ken-Ying Tseng and Rebecca Hsiao
Lee and Li, 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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The collection, processing and use of personal data by regulated entities were subject to the Computer-processed Personal Data Protection Act (CPDPA) and its Enforcement Rules promulgated by the Ministry of Justice (MoJ). Regulated entities include all government agencies and the following entities in the private sector:

- credit investigation agents and entities or individuals whose main business is the collection of personal data;
- hospitals;
- schools;
- telecommunications businesses;
- banks and other financial entities;
- securities businesses;
- insurance companies;
- publishing and broadcasting companies; and
- any other entities designated by the competent authorities.

On 27 April 2010, the legislature passed a bill to amend and rename the CPDPA the 'Personal Data Protection Act' (PDPA). On 26 May 2010, the registration requirements under the CPDPA were abolished along with the President's promulgation of the PDPA. Other provisions (except for articles 6 and 54, explained below) under the PDPA and the MoJ's amended Enforcement Rules took effect on 1 October 2012 and apply to anyone who collects, processes or uses personal data.

Article 6 of the PDPA prohibits the collection, processing and use of sensitive data, unless any exemption condition is met. Since the exemption conditions are too limited to meet certain industries' needs, the Executive Yuan had proposed a draft bill to amend article 6 to include other exemption conditions.

Article 54 of the PDPA requires that, within one year of the effective date of the PDPA, data owners must notify data subjects of the notification information under the PDPA, if the data owners had obtained the data subjects' personal data indirectly before the effective date of the PDPA. Considering that certain industries that own a large quantity of personal data are not capable of meeting the notification requirement within the one-year period, the Executive Yuan had proposed a draft bill to amend article 54 so that data owners must meet the notification requirement no later than the first time they use such personal data to contact the data subjects. The draft bill is pending the legislature's reading.

The amended articles 6 and 54 of the PDPA passed the legislature's third reading on 15 December 2015 and took effect on 15 March 2016 (amended PDPA).

The PDPA is a general law regulating the collection, processing and use of personal data. If there is any special law regulating the collection, processing and use of personal data, the special law should apply.

Under the PDPA, data owners are referred to as government agencies and non-government agencies (private sector). The PDPA imposes civil and criminal liabilities on government agencies, and imposes civil, criminal and administrative liabilities on non-government agencies if they illegally collect, process or use personal data. The civil liabilities relate to tortious acts. Since personal data involves a data subject's privacy, a data subject whose privacy is impinged upon may also claim damages against a government agency pursuant to the State Compensation Act and against a non-government agency pursuant to the Civil Code.

The PDPA has incorporated some provisions under Directive 95/46/EC. In addition, the MoJ has published some introductions on the OECD guidelines and the APEC Privacy Framework as references for various industries and data protection authorities to implement the PDPA.

2 Data protection authority

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

The MoJ is in charge of establishing the Enforcement Rules to the PDPA, which define and clarify, among others:

- terms under the PDPA;
- a data owner's obligations to supervise a commissioned agency;
- proper security measures;
- what constitutes a written consent and a proper notification; and
- how a data subject exercises rights.

The MoJ also answers questions from various government agencies and non-government agencies regarding how to interpret and comply with the PDPA. The MoJ's interpretations cannot bind the courts, but would usually be referred to and adopted by the courts in making judgments.

The enforcement of the PDPA is administered by the central and local (city and county) government authorities, which supervise the business operations of non-government agencies. The central government authorities may impose restrictions on a non-government agency's cross-border transfers of personal data and designate certain non-government agencies to establish a plan to maintain the security of personal data files and how to dispose of those files after they cease business operations. In addition, the purposes of the collection, processing, and use and categories of personal data are designated jointly by the MoJ and the central government authorities.

Both the central and local government authorities have the power to carry out audits and inspections. To audit and inspect any non-compliance, they may access the premises of non-government agencies, require information, and copy and retain documents and other objects from non-government agencies.

3 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 administrative sanctions and orders. A government agency's breach of the PDPA is subject to its internal corrective and disciplinary measures and those imposed by its superior government agency. In addition, both the central and local government authorities (which administer the enforcement of the PDPA) have the power to impose rectification orders and administrative penalties on non-government agencies that breach any requirement under the PDPA.

The following breaches may lead to criminal penalties:

- the illegal collection, processing or use of personal data with an intent to make unlawful profit for oneself or a third party, or with an intent to damage the interest of another, causing injury to another (article 41 of the amended PDPA);
- failure to obey a central government authority's order imposing restrictions on cross-border transfers of personal data with an intent to make unlawful profit for oneself or a third party, or with an intent to damage the interest of another, causing injury to another (article 41 of the amended PDPA); and
- the illegal change or deletion of personal data files or employment of any other illegal means with an intent to make unlawful profit for oneself or a third party, or with an intent to damage the interest of another, thereby impeding the accuracy of personal data files and causing injury to another (article 42 of the PDPA).

Criminal offences can be prosecuted by an injured person or a public prosecutor upon an injured person's complaint. If the criminal offences under article 41 are committed or the criminal offences under article 42 are committed against a government agency, they can be prosecuted by a public prosecutor solely on his or her initiative.

Scope

4 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 the public and private bodies who collect, process or use personal data. The following activities are exempt from the application of the PDPA:

- the collection, processing or use of personal data by an individual in the course of a personal or family activity; and
- the collection, processing or use of audiovisual information in a public place or a public activity, which is not associated with any other personal data.

5 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 regulates the use of personal data for marketing purposes; it does not specifically deal with electronic marketing. Although electronic marketing is dealt with under the Guidelines Governing the Consumer Protection in E-Commerce promulgated by the Consumer Protection Committee, the legislature has not passed a law specifically regulating electronic marketing.

The interception of communications and the monitoring and surveillance of individuals are covered by the Communications Protection and Detection Act and the Criminal Code. Since an individual's communications and activities are personal data and involve privacy, the illegal interception of an individual's communications and the illegal monitoring and surveillance of an individual's activities also constitute breaches of the PDPA and are tortious acts under the Civil Code.

6 Other laws

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

The PDPA is the only legislation that specifically regulates personal data protection. There are many other laws and regulations that cover personal data. For example, the Act Governing the Freedom of Government Information regulates the disclosure by government agencies of government information that may contain personal data. The Financial Holding Company Act regulates sharing among a financial holding company's subsidiaries of their clients' basic and transaction information. The Pharmaceutical Affairs Act regulates the drug safety surveillance and reporting system that includes patients' personal data.

7 PII formats

What forms of PII are covered by the law?

The PDPA has extended its protection from personal data for computer-processing to all personal data regardless of whether they are in electronic records or manual files.

8 Extraterritoriality

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

Under the PDPA, data owners are referred to as government agencies and non-government agencies (private sector). The PDPA defines a 'non-government agency' broadly to include a natural person, a juristic person and an unincorporated association. Pursuant to the book Personal Data Protection Act's Interpretation and Practice, written by the officials of the MoJ, a non-government agency that is subject to the PDPA is limited to a Taiwanese national or an entity registered in Taiwan, such as a foreign company that has established a branch office in Taiwan. A non-government agency must comply with the PDPA when collecting, processing or using an individual's personal data within Taiwan or a Taiwanese national's personal data outside the territory of Taiwan.

In addition, the MoJ has issued a directive confirming that the collection, processing and use of an individual's personal data by a foreign national or entity within Taiwan is also subject to the PDPA, regardless of whether such foreign national or entity is registered in Taiwan.

9 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?

Except for the exemption activities described under question 4, all processing and use of personal data by data owners or their commissioned agencies (explained below) are covered under the PDPA.

The PDPA requires that data owners comply with the requirements under the PDPA. The persons who collect, process and use personal data under the commission and on behalf of data owners are called commissioned agencies; a commissioned agency's conduct will be deemed as the data owner's conduct. The Enforcement Rules of the PDPA require that commissioned agencies comply with the requirements applicable to the data owners. A data owner must duly supervise the commissioned agency to ensure the latter's compliance and is liable to data subjects for the commissioned agency's or its own non-compliance.

Legitimate processing of PII

10 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 PDPA sets out different grounds for the legitimate processing of personal data, depending on whether a data owner is a government agency or a non-government agency.

A government agency may process personal data if it is for specific purposes and:

- the processing is necessary for the performance of job duties provided by law;
- the data subject has given his or her consent; or
- the processing will not be detrimental to the interests of the data subject.

A non-government agency may process personal data if it is for specific purposes and:

- the processing is specifically permitted by law;
- the processor and the data subject have entered into or are negotiating a contract and the processor has adopted appropriate security measures;
- the data is already in the public domain due to disclosure by the data subject or in a legitimate manner;
- it is necessary for statistics-gathering or academic research by an academic research institution for the public interest, provided that any information sufficient to identify the data subject has been removed;

- the data subject has given his or her consent;
- it is necessary for the furtherance of public interest;
- the data has been collected from a source accessible to the collector unless the interest of the data subject takes priority over that of the collector or processor; or
- the processing will not be detrimental to the interests of the data subject.

11 Legitimate processing – types of PII

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

Article 6 of the amended PDPA sets out distinct grounds for the legitimate processing of sensitive data.

Sensitive data includes medical history, medical treatments, genealogy, sex life, health-check results and criminal records.

Article 6 of the amended PDPA prohibits processing of sensitive data unless:

- the processing is provided by law;
- the processing is necessary for a government agency's performance of its statutory duties or non-government agency's fulfilment of legal obligations, and appropriate security measures have been or will be adopted therefor;
- the data is already in the public domain due to disclosure by the data subject or in a legitimate manner;
- the processing is necessary for statistics-gathering or academic research by a government agency or academic research institution for medical, health or crime-prevention purposes, provided that any information sufficient to identify the data subject has been removed;
- the processing is necessary for assisting a government agency or non-government agency to perform its statutory duties and appropriate security measures have been or will be adopted therefor; or
- the data subject has given his or her written consent, provided that processing is still prohibited if the processing goes beyond the necessary extent of the specific purposes, or any other law prohibits the processing despite the written consent of the data subject, or the consent is obtained against the data subject's will.

Data handling responsibilities of owners of PII

12 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?

If a data owner collects personal data directly from a data subject, the data owner must inform the data subject of the following information at the time of collection:

(i) the identity of the data owner;
(ii) the purposes for which his or her data is collected;
(iii) the type of data collected;
(iv) the term, place and method of use and the persons who may use the data;
(v) the data subject's rights (explained in question 14); and
(vi) the consequences of his or her failure to provide the required personal data (article 8 of the PDPA).

If a data owner collects personal data indirectly from a data subject, the data owner must inform the data subject of the data source and information (i) to (v) above no later than the first time they use such personal data to contact the data subject (article 9 of the PDPA).

13 Exemption from notification

When is notice not required?

The notification requirement under article 8 is exempt if:

(i) it is specifically permitted by law;
(ii) the collection is necessary for the performance of job duties provided by law or the fulfilment of legal obligations;
(iii) notification will affect a governmental agency's performance of its job duties or a non-government agency's fulfilment of legal obligations;
(iv) notification will prejudice public interest;
(v) the data subjects already have such information; or
(vi) the collection is not for any profit-seeking purpose and will obviously not be detrimental to the interests of the data subject.

The notification requirement under article 9 is exempt if:

- any of the above exemption situations (i) to (v) exists;
- the data subject has disclosed such information by him or herself, or when the information has been publicised legally;
- the notification may not be made to the data subject or his or her legal representative;
- it is for the public interest and necessary for the purpose of statistics or academic research and the data has been processed to such an extent that the data subject cannot be identified; or
- the personal data is collected by the mass media for the purpose of news reporting in the public interest.

14 Control of use

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

A data subject has rights to access his or her data to check and review them, have a copy of the data, supplement or revise the data, demand the data owner to cease its collection, processing or use of the data, and demand the data owner to delete the data.

Unless the processing or use are necessary for the performance of job duties or fulfilment of legal obligations or the data subject has consented in writing to the processing or use, a data owner must cease the processing or use of personal data if the data subject disputes the accuracy of the data, and must delete or cease the processing or use of personal data if the purposes of processing or use no longer exist or the term of use expires.

15 Data accuracy

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

A data owner must ensure the accuracy of personal data and update or supplement personal data on its own initiative or upon the data subject's request.

If the failure to provide accurate personal data is attributed to a data owner, the data owner should notify the persons to whom the data was provided as soon as the data owner updates or supplements the data.

16 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 impose a specific amount of data that can be held or a retention period. A data owner may retain personal data when the purposes of processing or use exists or during the term of use. After that, it may retain the personal data if it is necessary for the performance of job duties or the fulfilment of legal obligations or the data subject has consented in writing to the same. The retention is deemed to be necessary for a data owner's performance of job duties or fulfilment of legal obligations if:

- the retention period provided by law or contract has not expired;
- the deletion will be detrimental to the interests of the data subject; or
- there is any other legitimate ground for the retention.

17 Finality principle

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

A data owner may use personal data only if it is for, and reasonably associated with, the specific and lawful purposes for which the personal data has been collected.

18 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?

A data owner may use personal data for a specific and lawful new purpose (ie, the purpose other than those for which the personal data has been collected) if:

Update and trends

The unauthorised disclosure of personal data via smartphones is a hot topic for the data protection authorities. According to media reports, the personal data contained in smartphones will be accessed by, and disclosed to, mobile manufacturers, mobile operators and APP service providers without the relevant data subjects' consent. Hence, the NCC has suggested that mobile manufacturers imbed appropriate security mechanisms in mobile phones in order to enhance the safety of data transmission.

Protection of consumers' personal data is another hot topic in the financial industry. On 9 January 2015, the FSC amended the Regulations Governing Joint Marketing Activities Among Subsidiaries of A Financial Holding Company. Under the amendment, the personal data of customers, which the subsidiaries of any financial holding company may share among themselves, is limited to consumers' names and addresses. Any other personal data may be shared only if the sharing is otherwise provided by law or by contract signed by consumers, or if consumers have given their written consent. The contract must provide a choice for consumers to tick to express their consent (or to not consent) to the sharing, and must list all the subsidiaries involved. If the holding company increases or decreases any of such subsidiaries afterwards, the change in the subsidiaries should be published on the website of the holding company or the websites of the relevant subsidiaries.

- such use is specifically permitted by law;
- it is necessary for the maintenance of national security or furtherance of public interest;
- it is to prevent any injury or damage to human life, body, freedom or property;
- it is to prevent any third person's material right or interest from being prejudiced;
- it is necessary for statistic-gathering or academic research by an academic research institution for the public interest, provided that any information sufficient to identify the data subject has been removed;
- it may benefit the data subject; or
- the data subject has given written consent after the data owner has notified the data subject of the following information:
  - what the other purposes are;
  - the scope of use; and
  - how the data subject's rights and interests will be affected if he or she chooses not to give consent.

Security

19 Security obligations

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

The PDPA requires a data owner to have in place appropriate measures to prevent personal data or their files from being stolen, altered, damaged, destroyed, lost or disclosed.

The Enforcement Rules to the PDPA require a data owner to adopt, and to procure its commissioned agency to adopt, technical and organisational measures that are reasonable and sufficient to protect personal data. Such measures are recommended to include the following:

- allocation of personnel to enforce the measures and sufficient resources;
- identification of the scope of personal data;
- a personal data risk valuation and management mechanism;
- mechanisms for prevention, notification and handling of accidents;
- internal management procedures for collection, processing and use of personal data;
- security management and personnel management;
- education and training;
- IT infrastructure security management;
- data security auditing mechanisms;
- maintenance of access records, track log files and relevant evidence; and
- continuous improvement on security and maintenance measures.

20 Notification of data breach

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

If personal data is stolen, leaked or altered, or the data subjects' interests may otherwise be compromised because of a data owner's failure to comply with the PDPA, the data owner must notify the data subjects of the incident and the remedies that the data owner has adopted as soon as the data owner has carried out an investigation of the incident.

Internal controls

21 Data protection officer

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

The PDPA requires that a government agency that holds personal data files must assign personnel to administer the security and maintenance of those files, but does not specify the legal responsibilities of such personnel.

The PDPA does not impose the same obligation on a non-government agency.

22 Record keeping

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

Although the PDPA does not expressly require a data owner to maintain internal records or establish internal processes or documentation, the Enforcement Rules to the PDPA recommend that the security measures that a data owner must adopt include data security auditing mechanisms and maintenance of access records, track log files, and relevant evidence.

Registration and notification

23 Registration

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

The registration requirements under the CPDPA were abolished along with the President's promulgation of the PDPA on 26 May 2010.

24 Formalities

What are the formalities for registration?

Not applicable (see question 23).

25 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 23).

26 Refusal of registration

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

Not applicable (see question 23).

27 Public access

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

Not applicable (see question 23).

28 Effect of registration

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

Not applicable (see question 23).

Transfer and disclosure of PII

29 Transfer of PII

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

The PDPA simply provides that a commissioned agency's conduct will be deemed as the data owner's conduct. Hence, a data owner's transfer of personal data to its commissioned agency will be deemed the internal processing by the data owner of the personal data and subject to the restrictions stipulated for the processing thereof. See question 9.

30 Restrictions on disclosure

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

The disclosure of personal data to a third party constitutes the use of the personal data and thus is subject to the restrictions stipulated for the use thereof. See questions 17 and 18.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The central government authorities may impose restrictions on a non-government agency's cross-border transfers of personal data if:

- the transfer would prejudice any material national interest;
- it is prohibited or restricted under an international treaty or agreement;
- the country to which the personal data is to be transferred does not afford sound legal protection of personal data, thereby affecting the interests of the data subjects; or
- the purpose of the transfer is to evade restrictions under the PDPA.

On 25 September 2012, the National Communications Commission issued an order prohibiting communications enterprises from transferring subscribers' personal data to mainland China on the grounds that the personal data protection laws in mainland China are still inadequate.

32 Notification of cross-border transfer

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

No. The transfer of personal data outside Taiwan does not require the transferor to notify or seek the authorisation from a supervisory authority.

33 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 cross-border transfers apply equally to the transfers made to a commissioned agency or a third-party data owner. They do not apply to onward transfers.

Rights of individuals

34 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 view a copy of their personal data. On request, a data owner must provide a copy thereof to the individual unless:

- it would be detrimental to national security, diplomatic or military secrets, economic interests as a whole, or any other material national interests;
- it would impede a government agency's performance of job duties; or
- it would be detrimental to the material interests of the data owner or a third party.

35 Other rights

Do individuals have other substantive rights?

Individuals also have the right to:

- access his or her data to check and review them;
- supplement or revise the data;
- demand the data owner to cease its collection, processing or use of the data; and
- demand the data owner to delete the data.

36 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 based on the amount of their actual loss that they have suffered as a result of the breach of the PDPA by a data owner. They are also entitled to monetary compensation for distress if any of their intangible rights (eg, privacy and reputation) are damaged. The courts may set the amount of damages at NT$500 to NT$20,000 for each incident per person if an individual cannot prove the amount of actual damages or compensation.

37 Enforcement

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

If a government agency rejects an individual's request relating to any of the rights described under questions 34 and 35, the individual may file an administrative appeal with a supervisory authority of the government agency and if the appeal is dismissed, file an administrative complaint with a High Administrative Court to enforce his or her right. If a non-government agency rejects such request, the individual may file a civil complaint with a district court to enforce his or her right.

Individuals must file a civil complaint with a district court to claim monetary damages or compensation described under question 36.

理律法律事務所
LEE AND LI
ATTORNEYS-AT-LAW

Ken-Ying Tseng **kenying@leeandli.com**
Rebecca Hsiao **rebeccahsiao@leeandli.com**

7F, 201 Tun Hua N Road
Taipei 10508
Taiwan

Tel: +886 2 2715 3300
Fax: +886 2 2713 3966
www.leeandli.com

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

No.

Supervision

39 Judicial review

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

A government agency may not appeal against orders of its supervisory authority. A non-government agency will receive orders from a data protection authority described in question 2 and may appeal against such orders to the data protection authority's supervisory authority. If the appeal is dismissed, they may file an administrative complaint with a High Administrative Court.

Specific data processing

40 Internet use

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

The PDPA does not contain specific rules regarding cookies or equivalent technology. To the extent the use of such technologies involves the collection, processing or use of personal data, the requirements relating to the collection, processing or use under the PDPA will apply.

41 Electronic communications marketing

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

Sending marketing information by email, fax or telephone to data subjects constitutes the use of their personal data. A non-government agency must comply with the requirements relating to the use of personal data described under questions 17 and 18 (eg, a data subject has consented in a contract or given a separate consent) when it sends marketing information to data subjects (opt-in rules). A non-government agency must immediately cease the use of personal data for such marketing purposes if the data subject has notified the non-government agency that he or she does not wish to receive such marketing information (opt-out rules).

42 Cloud services

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

Taiwan does not have specific rules or regulator guidance on the use of cloud computing services. Processing personal data in the cloud is permitted, so long as it complies with the general requirements relating to the processing of personal data under the PDPA.

Turkey

Ozan Karaduman and Bentley James Yaffe
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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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. Besides 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 recent 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.

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 Data Protection Authority (DPA). It should be noted that, as of the date of writing, the Turkish DPA has not yet been established; with the temporary provision of the DPL stating that the authority will be established by 7 October 2016.

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.

As the Turkish DPA has not yet been established and the required ancillary data protection regulations have not yet been published, it is currently unknown how these investigative powers shall be applied.

3 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.

These breaches can be sanctioned with administrative fines ranging from 5,000 liras 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

4 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.

5 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 and the Regulation on Determination, Tapping, Recording of Telecommunication and Evaluation of Signal Information and the Formation of TIB.

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.

6 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, due 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 too.

The Social Security Institution, the public body authorised to oversee Turkey's reimbursement and social healthcare system, also has its own internet guidelines regarding the sharing of health data of which it is in possession.

7 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.

8 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.

9 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?

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, categorization 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.

Legitimate processing of PII

10 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 of the DPL is that the processing of personal data is only lawful if the relevant data subject has provided their explicit and informed consent. However, the Law itself also provides exceptions to this requirement of obtaining explicit and informed consent.

The exceptions to the requirement to obtain explicit consent for the processing of personal data are:
- processing is clearly mandated by laws;
- for a person who is unable to express their explicit consent due to a situation of impossibility, processing required for the safeguarding of their or a third person's life or physical wellbeing;
- processing is directly related to the formation or execution of an agreement to which the data subject is a party;
- processing is required for the data controller to satisfy their 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.

11 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

12 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.

13 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.

14 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 34–37, 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.

15 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.

16 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.

17 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 data controller chooses to base the processing.

18 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.

The only exception that can be said to apply to such new purposes is if the personal data in question is made anonymous by the data controller. As the provisions of the DPL do not apply to personal data that has been made anonymous and later used for such purposes as planning, statistics or research, this course of action would allow for use for new purposes.

Security

19 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. However, the DPL itself does not provide detailed explanations as to the content of these precautions.

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. It is expected that both the general technical and administrative precautions and the precautions specific to personal data of a sensitive nature will be among the first areas that will be detailed through ancillary regulations once the Turkish DPA begins operations.

The 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.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and 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'. As the DPL only recently came into effect, there have been no ancillary regulations to clarify and no details of areas such as breach notification processes.

Internal controls

21 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.

22 Record keeping

Are owners 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, it is likely that some form of documentation obligation will be introduced with the ancillary regulatory measures that detail the security measures and precautions that have been stated quite generally within the DPL.

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 obligation to maintain records that document access made to personal data and other related systems for a period of two years.

Registration and notification

23 Registration

Are PII owners and/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 Data Controller Register (the Register). It should be noted that the implementation of the provision detailing the requirement of registration has been delayed until 7 October 2016.

The Turkish DPA has not yet been established and the ancillary legislation detailing the registration process has not yet been drafted. Therefore, while the DPL does provide for the Turkish DPA to introduce exemptions for registration to the Register based on such considerations as the quality, amount and grounds of the processing, the content of the exemptions will be determined only after the Turkish DPA is established and issues a regulation in this regard.

However, 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.

24 Formalities

What are the formalities for registration?

As stated in the response to question 23, the more detailed requirements of registration to the Register will be determined once the Turkish DPA issues a regulation in that regard. However, the relevant provision of the DPL does establish the general principles relating to registration with the Register.

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, their 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.

25 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 Register or fails to maintain their registration with up-to-date information, said controller can be sanctioned with an administrative fine ranging from 20,000 liras to 1 million liras.

26 Refusal of registration

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

Currently the DPL does not provide any specific ground on which the Turkish DPA could refuse to allow an entry on the Register. In order to register with the Register, 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.

27 Public access

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

Yes, the DPL sets forth that the Register will be open to the public. However, for the reasons stated above, the current specifics of access and presentation have not yet been clarified by the Turkish DPA.

28 Effect of registration

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

No. Currently, the DPL does not explicitly attach any specific legal effect to entry onto the Register.

Transfer and disclosure of PII

29 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.

30 Restrictions on disclosure

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

Other than adhering to the requirement of either 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.

31 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. 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 following further approval and authorisation by the Turkish DPA.

A general restriction that applies to 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.

32 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.

33 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

34 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.

35 Other rights

Do individuals have other substantive rights?

In addition to the rights explained in our response to question 34, 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.

Update and trends

As the DPL is a fairly recent legislative measure, the currently anticipated updates in this area all relate to key areas of implementation becoming clearer once the Turkish DPA begins operations and the provisions that were delayed until 7 October 2016 come into effect.

36 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.

37 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

38 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 4, 13, 24 and 34, there are no further exemptions or limitations on the application of the provisions of the DPL.

Supervision

39 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

40 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.

41 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.

42 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 is currently 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 transfer can also be applied to situations where cloud computing services are obtained from companies with servers abroad.

GÜN + PARTNERS
AVUKATLIK BÜROSU

Ozan Karaduman **ozan.karaduman@gun.av.tr**
Bentley James Yaffe **james.yaffe@gun.av.tr**

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
Istanbul
Turkey

Tel: +90 212 354 00 00
Fax: +90 212 274 20 95
www.gun.av.tr

United Kingdom

Bridget Treacy
Hunton & Williams

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The primary legal instrument is the Data Protection Act 1998 (DPA), which implements Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of PII and the free movement of data. It is supported by secondary legislation made by statutory instrument, for example, setting fee levels for access rights. The United Kingdom has incorporated the Convention rights under the European Convention on Human Rights into law in the Human Rights Act 1998 and some privacy rights have been developed by the courts as a result of the application of that Act. 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.

At the time of writing, the future of the UK's data protection law is uncertain. In a referendum held on 23 June 2016, the UK voted to leave the EU. The formal mechanism by which the UK would leave has not yet been triggered, nor is it clear 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 adopt EU laws, including the EU General Data Protection Regulation (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). Further, non-EU controllers or processors who 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. Accordingly, for now, UK organisations are likely to continue their preparations for the implementation of the GDPR on 25 May 2018, but the position should be kept under review.

2 Data protection authority

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

The DPA is supervised by the Information Commissioner's Office (ICO) appointed under the DPA. 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 mandatory audit (referred to as 'assessment');
- conduct audits of private sector organisations with the consent of the organisation;
- impose mandatory orders on data owners (those who control PII, known as 'data controllers' under the DPA) requiring them to take such steps as he or she sets out in the order; and
- impose fines of up to £500,000 for serious breaches of the DPA.

All of the orders made by the ICO may be appealed. The ICO also has specific powers under secondary legislation dealing with electronic marketing to make orders in relation to notice of breaches of security by providers of electronic communication services.

3 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 number of breaches may lead to criminal penalties. The following may constitute criminal offences:

- failure by a data owner, where required, to register and maintain an accurate entry in the register;
- failure to comply with a mandatory enforcement or information notice under the DPA within the specified time; and
- obstructing execution of a warrant of entry, failing to cooperate or providing false information.

Further, a person who procures the disclosure of PII or discloses PII without the consent of the data owner or sells or offers for sale PII obtained without such permission commits a criminal offence.

Criminal offences can be prosecuted by the ICO or by or with the consent of the Director of Public Prosecutions.

Scope

4 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 DPA applies to public and private sector bodies.

5 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 DPA often applies to the same activities, to the extent that they involve the processing of PII. The retention of PII by electronic service providers is regulated by the Data Retention (EC Directive) Regulations 2009. Interception and state surveillance are covered by the Regulation of Investigatory Powers Act 2000. The interception of business communications is regulated by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 made under the Regulation of Investigatory Powers Act 2000.

6 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.

A code of practice made under the DPA applies to the sharing of PII between data owners.

7 PII formats

What forms of PII are covered by the law?

The DPA covers 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.

8 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 owners 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 European Economic Area (EEA) but make use of a 'means' of processing in the UK to process PII (other than for purposes of mere transit of PII through the UK). A 'means' of processing includes equipment used to process PII, or a 'data processor'. A 'data processor' is an organisation that carries out outsourced processing of PII on behalf of a data owner.

A data owner 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 an office, branch, agency or other regular practice in the UK.

Data owners established outside the UK but using a means of processing in the UK are obliged to nominate a representative in the UK.

9 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?

The DPA is applicable to data owners only (ie, those that decide the means and purposes of the data processing). Data processors (who merely process PII at the behest of data owners) have no direct legal obligations under the DPA.

Legitimate processing of PII

10 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 DPA sets out different grounds for legitimate processing depending on whether the PII are non-sensitive or sensitive.

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 owner (or third parties to whom the PII is disclosed), unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

11 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;
- commission or alleged commission of any offence; or
- any proceedings for committed or alleged offences, the disposal of such proceedings of sentence of any court.

The grounds for processing sensitive PII include:

- explicit consent of the individual;
- performance of employment law obligations;
- 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.

The DPA does not impose any sector-specific rules.

Data handling responsibilities of owners of PII

12 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 owners are obliged to notify individuals of:

- the data owner's identity;
- its nominated representative in the UK (if applicable);
- the purposes for which the PII will be processed; and
- any further information required to make the processing fair.

Examples of such further information are unexpected uses of the PII, third-party disclosures and transfers to third countries not offering adequate protection.

Where the PII is collected directly from the individual, notice is required 'so far as practicable' and must be provided at the time of collection. Where the PII is obtained from another source, notice must be provided at the time of (or as soon as practicable thereafter) the data owner first processing the PII, or disclosure to a third party being envisaged.

13 Exemption from notification

When is notice not required?

Where PII is obtained from a third party and is required for a statutory purpose, or the provision of notice would involve disproportionate effort, notice is not required as long as the individual has not previously signified in writing that he or she requires a notice. A PII owner that relies upon this provision relating to disproportionate effort must keep a record of the fact.

14 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 rights of access, amendment and objection. A data owner must provide the individual with a copy of the PII it holds on him or her upon request. Individuals may request amendment of inaccurate data, and may object to processing where it is likely to cause substantial unwarranted damage or distress. Further, individuals may object at any time to the processing of their PII for the purposes of direct marketing.

15 Data accuracy

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

The data owner must ensure that PII is relevant, accurate and, where necessary, kept up to date in relation to the purpose for which it is held.

16 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 owner 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 owner should not collect or process unnecessary or irrelevant PII. The DPA does not impose any specified retention periods. PII may only be held as long as is necessary for the purposes for which it is processed.

17 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 may be specified in the notice given to the individual or the registration lodged with the ICO.

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 owner, independent of any action taken under the DPA.

18 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 10). 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 (non-disclosure 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

19 Security obligations

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

The DPA does not specify the types of security measures that data owners must take in relation to PII. Instead, the DPA states that data owners 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]'.

Under the relevant provisions, in assessing what is 'appropriate' in each case, data owners 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 owner must take reasonable steps to ensure the reliability of its employees.

Where a data owner uses an outsourced provider of services to process PII it must chose a 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 or evidenced in writing under which the processor will act only on the instructions of the owner and apply equivalent security safeguards to those imposed on the data owner.

20 Notification of data breach

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

There is no obligation in the DPA on data owners to report data breaches either to the ICO or to the affected individuals; however, government departments have been instructed to report breaches and the ICO has issued 'best practice' guidance, advising other data owners to determine whether a breach is sufficiently serious to warrant reporting based on a range of factors, including the number of individuals affected, the nature of the data and whether the breach was malicious in nature. The ICO does not expect every breach to be reported, and small breaches should be dealt with by the relevant data owner. Providers of electronic communication services are obliged to report some types of breach.

In most circumstances, a data processor that suffers a data breach would be expected (under the terms of a well-drafted data processing agreement) to notify the data owner of that breach. The data owner then would decide, in accordance with the principles set out above, whether to report that breach.

Internal controls

21 Data protection officer

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

There is no legal requirement to appoint a person to the role of 'data protection officer', but many organisations do appoint such officers. The role will generally cover, at a minimum, the maintenance of the organisation's registration and the handling of enquiries and requests from individuals.

22 Record keeping

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

Where a data owner takes advantage of an exemption from the obligation to register its data processing with the ICO, it may be obliged to provide an enquirer with a written statement describing the processing being carried out. A record must be kept of any decision to rely on the provision in relation to disproportionate effort as described in question 13. There are no other specific obligations to retain internal records or maintain internal processes; however, the DPA requires that PII shall be 'adequate, relevant and not excessive', and 'shall be accurate and, where necessary, kept up to date'. Data owners may need to maintain internal records and establish internal processes or documentation to satisfy these requirements in practice. In addition, where a data owner makes a decision that may later be queried by an individual or the ICO, it is advisable for the data owner to keep clear records of that decision and the reasons for it. For example, where a data owner makes its own adequacy determination for the purposes of data transfers (see question 31) it should keep a record of that determination and the information that gave rise to it.

Registration and notification

23 Registration

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

Data owners are required to register with the ICO, but several exceptions exist. There is no obligation to register 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 owner 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 owner 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 (and not a data owner) is not required to register.

24 Formalities

What are the formalities for registration?

There is a two-tier registration fee structure. The higher-tier fee, currently set at £500, applies to data owners that either:

- have a turnover of £25.9 million and at least 250 members of staff; or
- are a public authority with at least 250 members of staff.

All other data owners (including all registered charities and small occupational pension schemes) fall into in the lower-tier category, paying £35, unless they are exempt. The registration period is one year, and the registration expires at the end of that period unless it is renewed.

The data owner must include in the registration application its name, address, and a description of the relevant processing, the purposes of that processing, details of third-party recipients of the relevant PII and information about transfers outside the UK, as well as a general description of the security measures it has in place. Once registered, a data owner is responsible for ensuring that the registration details are kept up to date.

25 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 owner is currently registered with the ICO and, once registered, keeps its registration details up to date.

If the data owner is not registered or fails to maintain an accurate entry in the register, the data owner is guilty of a criminal offence that could lead to an unlimited fine. As previously noted, an entity that is a data processor only (and not a data owner) is not required to register.

26 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 an application for registration provided that it is made in the prescribed form and includes the applicable fee. An entry that contains inaccurate content or statements may be rejected by the ICO as an invalid application, but there is no power to refuse a valid application.

27 Public access

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

The 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.

28 Effect of registration

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

An entry on the register does not cause the data owner to be subject to obligations or liabilities to which it would not otherwise be subject.

The data owner's entry on the register must specify the purposes for which the PII will be processed. If those purposes change, the data owner must update the information on the register (there is no fee for updating the register).

There is no obligation to give notice to individuals in connection with the registration of the data owner.

The contents of the entry have the effect of specifying the purposes of the processing, but notice must also be provided to individuals of the processing.

Transfer and disclosure of PII

29 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 'data processors' under the DPA. Data processors do not have direct legal obligations under the DPA in respect of the PII that they process as outsourced service providers. The obligation to ensure that the processor processes PII in accordance with the DPA rests with the data owner. The data owner 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 owner 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 owner and to apply security controls and standards that meet those required by the DPA.

30 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 owner or procure the disclosure of PII to another party without the consent of the data owner. 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 the disclosure of PII obtained in the course of their functions other than in accord with those functions.

There are no other specific restrictions on disclosure of PII, other than compliance with the general principles described earlier, and the cross-border restrictions as set out in question 31.

31 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.

Data owners in the UK are entitled to make their own determination of adequacy in relation to a jurisdiction to which PII will be transferred. In assessing the adequacy of such a jurisdiction, the data owner should take into account a variety of factors, including the nature of the PII, the law in force in the country of destination, and security measures taken in relation to the data and the purposes of the processing.

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 owner 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;
- 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 'Safe Harbor'. 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.

32 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. A description of overseas transfers must be included on the register (see question 24).

33 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 owners.

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

34 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. A request must be in writing and a small fee is payable. Within 40 days of receipt of a valid request the data owner 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 of the PII, together with a copy of the PII in an intelligible form and any information available to the owner as to the sources of the PII.

A data owner must be satisfied as to the identity of the individual making the request. A data owner does not have to provide third-party data where that would breach the privacy of the third party and may reject repeated identical requests.

In some cases the data owner may withhold PII to protect the individual, for example, where health data are involved, or to protect other important specified public interests such as the prevention of crime. All such exceptions are specifically delineated in the law.

35 Other rights

Do individuals have other substantive rights?

Individuals have the following further rights:

- to object to the processing of PII for the purposes of direct marketing;
- to object to the processing of PII that would cause substantial unwarranted damage or distress;
- to restrict the taking of automated decisions in a limited number of cases; and
- to seek rectification or erasure or blocking of PII where the data are inaccurate.

36 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 damage as a result of the contravention of the DPA by a data owner. Where an individual is entitled to compensation for damage they may also seek compensation for any associated distress. In the absence of pecuniary damage, the DPA indicates that mere distress or injury to feelings is not a basis for compensation. However, recent case law has clarified that damages for distress or injury to feelings may be granted in some cases. Where the contravention relates to the purposes of journalism or the production of literary or artistic works, compensation may be awarded for distress alone.

37 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 34–36.

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.

Update and trends

The most significant UK data protection development is the uncertainty created by the result of the recent referendum in which the UK decided to leave the EU (described in question 1). It will take some time before the implications of this become clear.

In addition, Information Commissioner Christopher Graham stepped down from office on 28 June 2016, and will be replaced by Elizabeth Denham, formerly the Privacy and Information Commissioner for British Colombia, Canada. During her pre-appointment hearing, Ms Denham stated her willingness to levy heavy fines for serious breaches of data protection law, but advocated a regulatory approach that prioritises proactive guidance, advice and education to those involved in data processing activities.

Other hot topics in the UK include the fallout from the Court of Justice of the European Union's decision in *Schrems*, which invalidated the Safe Harbor and has created a degree of uncertainty as to the future validity of other data transfer mechanisms, including Model Clauses. Attention is focused on the recently introduced Privacy Shield, following its approval as a replacement for Safe Harbor. Significant attention is also focussed on the GDPR. See the EU Overview for further discussion of the Privacy Shield and GDPR.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

The DPA 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.

As noted in question 23, some forms of processing of PII are exempt from the obligation to register the processing on the public register.

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

39 Judicial review

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

Data owners 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

40 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. Such consent is not, however, required where the information is:

- only used for transmission of communications over electronic communications networks; or
- strictly necessary for the provision of a service requested by the user.

The ICO has recognised that in some circumstances, it may be impractical to obtain consent before a cookie is placed and subsequent validation may be the only option.

41 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.

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 who 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.

42 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 owners 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& WILLIAMS

Bridget Treacy **btreacy@hunton.com**

30 St Mary Axe
London EC3A 8EP
United Kingdom

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

United States

Lisa J Sotto and Aaron P Simpson
Hunton & Williams

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The US legislative framework for the protection of PII resembles a patchwork quilt. Unlike other jurisdictions, the US does not have a dedicated data protection law, but instead regulates 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) against covered entities.

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 decree.

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 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

4 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.

5 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. 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.

6 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.

7 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. 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 hardcopy records.

8 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.

9 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?

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

10 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.

11 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.

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.

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.

Data handling responsibilities of owners of PII

12 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.

Delaware also has enacted a law, the Delaware Online and Privacy Protection Act, that requires operators of commercial internet services to provide similar information to their users when collecting PII online. In addition to the California and Delaware 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, pre-screened 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.

13 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.

14 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.

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.

15 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).

16 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.

17 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.

18 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

19 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 national 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 licence 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.

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.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and 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, 47 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

21 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. Many organisations in the US appoint a Chief Privacy Officer, but his or her responsibilities are dictated by business need rather than legal requirements.

22 Record keeping

Are owners 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 19, 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.

Registration and notification

23 Registration

Are PII owners and/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.

24 Formalities

What are the formalities for registration?

There are no registration requirements for data processing activities in the US.

25 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.

26 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.

27 Public access

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

There are no registration requirements for data processing activities in the US.

28 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.

Transfer and disclosure of PII

29 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.

30 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.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

US privacy laws do not impose restrictions on cross-border data transfers.

32 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.

33 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

34 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.

35 Other rights

Do individuals have other substantive rights?

There are no laws of general application in the US that provide individuals with other substantive rights. Some sector-specific laws provide such 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.

36 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. Pursuant to the FCRA, for example, 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.

37 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

38 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.

Supervision

39 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

40 Internet use

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

As of August 2016, this is a hot-button issue in the US, and regulation is evolving rapidly. 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 have 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.

41 Electronic communications marketing

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

See question 5.

42 Cloud services

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

There are no rules or regulator guidance specific to the use of cloud computing services.

HUNTON& WILLIAMS

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

200 Park Avenue
New York
New York 10166
United States

Tel: +1 212 309 1000
Fax: +1 212 309 1100
www.hunton.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Construction
Copyright
Corporate Governance
Corporate Immigration
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
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
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

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law