DATA PROTECTION LAWS OF THE WORLD

DLA PIPER

TABLE OF CONTENTS

ABSTRACT

More than ever it is crucial that organisations manage and safeguard personal information and address their risks and legal responsibilities in relation to processing personal data, to address the growing thicket of applicable data protection legislation.

A wellconstructed and comprehensive compliance program can solve these competing interests and is an important riskmanagement tool.

This handbook sets out an overview of the key privacy and data protection laws and regulations across nearly 100 different jurisdictions and offers a primer to businesses as they consider this complex and increasingly important area of compliance.

DLA Piper's global data protection and privacy team has the deep experience and international reach to help global businesses develop and implement practical compliance solutions to the myriad data protection laws that apply to global businesses.

INTRODUCTION

Welcome to DLA Piper's Data Protection Laws of the World Handbook. We launched the first edition of the handbook in 2012, and following such a positive response have been updating it annually ever since.

We continue to witness a period of unprecedented activity in the development of data protection regulation around the world which will have a profound impact on the way in which global businesses are required to approach the collection and management of personal information.

These changes are being driven largely by cultural and trade considerations and by a struggle to keep pace with emerging technology and online business methods. At an EU level, political agreement has finally been reached on the General Data Protection Regulation, and the final text should be formally adopted early this year. Of equal significance is the toughening of legal requirements and of enforcement in countries such as Korea, Hong Kong and Singapore. Furthermore, the emergence of laws in countries which previously had no data protection law in place, including a large number of countries in Asia, Latin America and the Middle East, continues and could create considerable enforcement risk in the future.

Should you require further guidance, please do not hesitate to contact us at **dataprivacy@dlapiper.com**.

DATA PRIVACY SCOREBOX

You may also be interested in our Data Privacy Scorebox, a tool to help you assess your data protection strategy. It requires completing a survey covering 12 areas of data privacy, such as storage of data, use of data, and customers' rights. Once completed, a report summarising your organisation's alignment with key global principles of data protection is produced. The report includes a visual summary of the strengths and weaknesses of your data protection strategy, a practical action point check list, as well as peer benchmarking data.

To access the Scorebox, please visit www.dlapiper.com/dataprotection

CYBERTRAK

We are pleased to introduce CyberTrak, an innovative online cybersecurity tool featuring information on cybersecurity-related mandates in 23 key markets around the world. CyberTrak is the inaugural product of a partnership between Blue Edge Lab^{SM*} and the Internet Security Alliance (ISA).

CyberTrak provides multinational companies instant online access to critical information about cybersecurity-related laws, regulations and generally accepted standards in 23 key markets in the Americas, Asia-Pacific, Europe and the Middle East and in four highly regulated sectors in the US. It also provides brief summaries of requirements, as well as

an assessment on enforcement risk and the degree of activity triggering the requirement.

Cybersecurity laws and regulations are evolving rapidly around the world. Companies battling ever more sophisticated cyberattacks face mounting compliance costs and higher risks if they do not keep up with new requirements in all markets where they operate.

CyberTrak is designed to help GCs, CIOs, CISOs, risk officers and legal, technology, IT and procurement departments of multinational companies make better, faster risk management decisions and reduce the costs associated with keeping up with these changing regulatory requirements.

CyberTrak content will be regularly updated three times per year by a global group of more than 50 carefully selected contributors in key jurisdictions (many of them contributors to Data Protection Laws of the World), along with interim updates when major changes occur.

Understanding cybersecurity mandates on a global scale is critical to any multinational company that collects and retains customer data, trade secrets, and other confidential data or operates in a critical infrastructure sector, such as energy, financial services, healthcare and defense/government contractors.

Company-wide CyberTrak access is offered on an annual subscription basis. To register for a free trial or to learn more about CyberTrak, please visit **www.BlueEdgeLab.com**.

**Blue Edge Lab, LLC is a wholly owned subsidiary of DLA Piper LLP (US). Blue Edge Lab is not a law firm and does not provide legal services.*

DATA PROTECTION BLOG

If you find this Handbook useful, you may also be interested in DLA Piper's Data Protection, Privacy and Security group's Privacy Matters Blog − a blog featuring regular data protection, privacy and security legal updates to help you remain aware of the most important legal and regulatory developments.

We have over 130 experienced privacy and security lawyers across the globe who are close to the regulations in each of their respective jurisdictions and who regularly post summary articles on their local issues.

To access the blog, please visit **http://blogs.dlapiper.com/privacymatters/**

To ensure you receive an automatic email when a new article is posted, please enter your details in the 'subscribe' section found on the blog's righthand sidebar.

DISCLAIMER

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Furthermore, enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

I. INTRODUCTION

EU data protection legislation is facing huge changes. Data protection laws are built on fundamental rights enshrined in the Charter of Fundamental Rights of the European Union which are the core building blocks of the EU's legal regime. Privacy issues arising from an exponential growth in consumer and mobile technologies, an increasingly connected planet and mass cross border data flows have pushed the EU to entirely rethink its data protection legislation to ensure that these fundamental rights are fully protected in today's digital economy.

In 2012, the European Commission published a draft regulation (the General Data Protection Regulation, 'GDPR'). Just over four years later, the final text of GDPR was published in the Official Journal of the European Union on 27 April 2016. Regulation 2016/679heralds some of the most stringent data protection laws in the world and shall apply from 25 May 2018.

The current EU Data Protection Directive (95/46/EC) was adopted in 1995. It has been implemented differently by EU Member States into their respective national jurisdictions, resulting in the fragmentation of national data protection laws within the EU. As it is a Regulation, GDPR will come into effect immediately on 25 May 2018 without any need for additional domestic legislation in EU Member States. However, with more than 30 areas where Member States are permitted to legislate (differently) in their domestic laws there will continue to be significant variation in both substantive and procedural data protection laws among the EU's different Member States.

The clock is now ticking with fines of up to 4% of total worldwide annual turnover for failing to comply with the requirements of GDPR. Organisations have a great deal to do between now and 25 may 2018 to be ready for the new regime

II. CURRENT SITUATION

At present, personal data processed in the European Union is governed by the 1995 European 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 (Directive). The Directive establishes a number of key legal principles:

- Fair and lawful processing
- Purpose limitation and specification
- Minimal storage term
- Transparency
- Data quality
- Security
- Special categories of data
- Data minimisation

These principles have been implemented in each of the 28 European Union Member States through national data protection law. Although all originating from the same core Directive, there is significant variation among Member State's substantive and procedural data protection laws.

III. FUTURE LEGAL FRAMEWORK

After almost four years of often fractious negotiations, GDPR was published in the Official Journal of the European Union as Regulation 2016/679 on 27 April 2016.

There will be a two year transition period to allow organisations and governments to adjust to the new requirements and procedures. Following the end of this transitional period, the Regulation will be directly applicable throughout the EU from 25 May 2018, without requiring implementation by the EU Member States through national law.

The goal of European legislators was to harmonise the current legal framework, which is fragmented across Member States. A 'Regulation' (unlike a Directive) is directly applicable and has consistent effect in all Member States, and

GDPR was intended to increase legal certainty, reduce the administrative burden and cost of compliance for organisations that are active in multiple EU Member States, and enhance consumer confidence in the single digital marketplace. However, in order to reach political agreement on the final text there are more than 30 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws. There continues to be room for different interpretation and enforcement practices among the Member States. There is therefore likely to continue to be significant differences in both substantive and procedural data protection laws and enforcement practice among EU Member States when GDPR comes into force.

We have summarised the key changes that will be introduced by the GDPR in the following sections

Key changes to the current data protection framework include:

A. WIDER TERRITORIAL SCOPE

Where organisations are established within the EU

GDPR applies to processing of personal data “in the context of the activities of an establishment” (Article 3(1)) of any organization within the EU. For these purposes “establishment” implies the “effective and real exercise of activity through stable arrangements” (Recital 22) and “the legal form of such arrangements…is not the determining factor” (Recital 22), so there is a wide spectrum of what might be caught from fully functioning subsidiary undertakings on the one hand, to potentially a single individual sales representative depending on the circumstances.

Europe’s highest court, the Court of Justice of the European Union (the CJEU) has been developing jurisprudence on this concept, recently finding (*Google Spain SL, Google Inc. v AEPD*, *Mario Costeja Gonzalez* (C-131/12)) that Google Inc with EU based sales and advertising operations (in that particular case, a Spanish subsidiary) was established within the EU. More recently, the same court concluded (*Weltimmo v NAIH* (C-230/14)) that a Slovakian property website was also established in Hungary and therefore subject to Hungarian data protection laws.

Where organisations are not established within the EU

Even if an organization is able to prove that it is not established within the EU, it will still be caught by GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services" (Art 3(2)(a)) (no payment is required) to such data subjects in the EU or "the monitoring of their behaviour" (Art 3(2)(b)) as far as their behaviour takes place within the EU. Internet use profiling (Recital 24) is expressly referred to as an example of monitoring .

Practical implications

1. Compared to the current Directive, GDPR will capture many more overseas organisations. US tech should particularly take note as the provisions of GDPR have clearly been designed to capture them.

2. Overseas organisations not established within the EU who are nevertheless caught by one or both of the offering goods or services or monitoring tests must designate a representative within the EU (Article 27).

B. TOUGHER SANCTIONS

Revenue based fines

GDPR joins anti-bribery and anti-trust laws as having some of the very highest sanctions for non-compliance including revenue based fines of up to 4% of annual worldwide turnover.

To compound the risk for multinational businesses, fines are imposed by reference to the revenues of an undertaking rather than the revenues of the relevant controller or processor. Recital 150 of GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully the Treaty doesn’t define the term either and the extensive case-law is not entirely straightforward with decisions often turning on

the specific facts of each case. However, in many cases group companies have been regarded as part of the same undertaking. This is bad news for multinational businesses as it means that in many cases group revenues will be taken into account when calculating fines, even where some of those group companies have nothing to do with the processing of data to which the fine relates provided they are deemed to be part of the same undertaking. The assessment will turn on the facts of each case.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to 20,000,000 Euros or in the case of an undertaking up to 4% of total worldwide turnover of the preceding year, whichever is higher apply to breach of:

- the basic principles for processing including conditions for consent
- data subjects' rights
- international transfer restrictions
- any obligations imposed by Member State law for special cases such as processing employee data
- certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to 10,000,000 Euros or in the case of an undertaking up to 2% of total worldwide turnover of the preceding year, whichever is the higher apply to breach of:

- obligations of controllers and processors, including security and data breach notification obligations
- obligations of certification bodies
- obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Broad investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

GDPR makes it considerably easier for individuals to bring private claims against data controllers and processors. In particular:

- any person who has suffered "material or non-material damage" as a result of a breach of GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress and hurt feelings even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80). Although this falls someway short of a US style class action right, it certainly increases the risk of group privacy claims against consumer businesses. Employee group actions are also more likely under GDPR.

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or proessor (Article 79).

Practical implications

1. The scale of fines and risk of follow-on private claims under GDPR means that actual compliance is a must. GDPR is not a legal and compliance challenge – it is much broader than that, requiring organisations to completely transform the way that they collect, process, securely store, share and securely wipe personal data. Engagement of senior management and forming the right team is key to successful GDPR readiness.

2. GDPR will apply throughout the EU on 25 May 2018. Organisations caught by GDPR will need to map current data collection and use, carry out a gap analysis of their current compliance against GDPR and then create and implement a remediation plan, prioritizing high risk areas.

3. GDPR will require suppliers and customers to review supply chains and current contracts. Contracts will need to be renegotiated to ensure GDPR compliance and commercial terms will inevitably have to be revisited in many cases given the increased costs of compliance and higher risks of non-compliance.

4. The very broad concept of 'undertaking' is likely to put group revenues at risk when fines are calculated, whether or not all group companies are caught by GDPR or were responsible for the infringement of its requirements. Multinationals even with quite limited operations caught by GDPR will therefore need to carefully consider their exposure and ensure compliance.

5. Insurance arrangements will need to be reviewed and cyber and data protection exposure added to existing policies or purchased as stand-alone policies where possible. The terms of policies will require careful review as there is wide variation among wordings and many policies may not be suitable for the types of losses which are likely to occur under GDPR.

C. MORE DATA CAUGHT

Personal data is defined as "any information relating to an identified or identifiable natural person". (Article 4) A low bar is set for "identifiable" – if anyone can identify a natural person using “all means reasonably likely to be used” (Recital 26) the information is personal data, so data may be personal data even if the organisation holding the data cannot itself identify a natural person. A name is not necessary either – any identifier will do such as an identification number, location data, an online identifier or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30 with IP addresses, cookies and RFID tags all listed as examples.

Although the definition and recitals are broader than the equivalent definitions in the current Directive, for the most part they are simply codifying current guidance and case law on the meaning of 'personal data'.

GDPR also includes a broader definition of "special categories" (Article 9) of personal data which are more commonly known as sensitive personal data. The concept has been expanded to expressly include the processing of genetic data and biometric data. The processing of these data are subject to a much more restrictive regime.

A new concept of 'pseudonymisation' (Article 4) is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Organisations which implement pseudonymisation techniques enjoy various benefits under GDPR.

Practical implications

1. If in any doubt, it is prudent to work on the assumption that data is personal data given the extremely wide definition of personal data in GDPR.

2. GDPR imposes such a high bar for compliance, with sanctions to match, that often the most effective approach to minimise exposure is not to process personal data in the first place and to securely wipe legacy personal data or render it fully anonymous, reducing the amount of data subject to the requirements of GDPR.

3. Where a degree of identification is required for a specific purpose, the next best option is only to collect and use pseudonymous data. Although this falls within the regulated perimeter, it enjoys a number of benefits for organisations in particular that in the event of a data breach it is much less likely that pseudonymous data will cause harm to the affected individuals, thereby also reducing the risk of sanctions and claims for the relevant organisation.

4. Organisations should only use identifiable personal data as a last resort where anonymous or pseudonymous data is not sufficient for the specific purpose.

D. SUPPLIERS (PROCESSORS) CAUGHT TOO

GDPR directly regulates data processors for the first time. The current Directive generally regulates controllers (ie those responsible for determining the purposes and means of the processing of personal data) rather than 'data processors' - organisations who may be engaged by a controller to process personal data on their behalf (eg as an agent or supplier).

Under GDPR, processors will be required to comply with a number of specific obligations, including to maintain adequate documentation (Article 30), implement appropriate security standards (Article 32), carry out routine data protection impact assessments (Article 32), appoint a data protection officer (Article 37), comply with rules on international data transfers (Chapter V) and cooperate with national supervisory authorities (Article 31). These are in addition to the requirement for controllers to ensure that when appointing a processor, a written data processing agreement is put in place meeting the requirements of GDPR (Article 28). Again, these requirements have been enhanced and gold-plated compared to the equivalent requirements in the Directive.

Processors will be directly liable to sanctions (Article 83) if they fail to meet these criteria and may also face private claims by individuals for compensation (Article 79).

Practical implications

1. GDPR completely changes the risk profile for suppliers processing personal data on behalf of their customers. Suppliers now face the threat of revenue based fines and private claims by individuals for failing to comply with GDPR. Telling an investigating supervisory authority that you are just a processor won't work; they can fine you too. Suppliers need to take responsibility for compliance and assess their own compliance with GDPR. In many cases this will require the review and overhaul of current contracting arrangements to ensure better compliance. The increased compliance burden and risk will require a careful review of business cases.

2. Suppliers will need to decide for each type of processing undertaken whether they are acting solely as a processor or if their processing crosses the line and renders them a data controller or joint controller, attracting the full burden of GDPR.

3. Customers (as controllers) face similar challenges. Supply chains will need to be reviewed and assessed to determine current compliance with GDPR. Privacy impact assessments will need to be carried out. Supervisory authorities may need to be consulted. In many cases contracts are likely to need to be overhauled to meet the new requirements of GDPR. These negotiations will not be straightforward given the increased risk and compliance burden for suppliers. They will also be time consuming and it would be sensible to start the renegotiation exercise sooner rather than later, particularly as suppliers are likely to take a more inflexible view over time as standard positions are developed.

4. There are opportunities for suppliers to offer GDPR "compliance as a service" solutions, such as secure cloud solutions, though customers will need to review these carefully to ensure they dovetail to their own compliance strategy.

E. DATA PROTECTION PRINCIPLES

The core themes of the data protection principles in GDPR remain largely as they were in the Directive, though there has been a significant raising of the bar for lawful processing (see Higher Bar for Lawful Processing) and a new principle

of accountability has been added.

Personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle")
- Accurate and where necessary kept up to date (the "accuracy principle")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle").

Practical implications

1. Controllers will need to assess and ensure compliance of data collection and use across their organisations with each of the above principles as any failure to do so attracts the maximum category of fines of up to 20 million Euros / 4% of worldwide annual turnovers. Data mapping, gap analysis and remediation action plans will need to be undertaken and implemented.

2. The enhanced focus on accountability will require a great deal more papering of process flows, privacy controls and decisions made to allow controllers to be able to demonstrate compliance. See Accountability and Governance

F. HIGHER BAR FOR LAWFUL PROCESSING

The lawfulness, fairness and transparency principle amongst other things requires processing to fall within one or more of the permitted legal justifications for processing. Where special categories of personal data are concerned, additional much more restrictive legal justifications must also be met.

Although this structure is present in the Directive, the changes introduced by GDPR will make it much harder for organisations to fall within the legal justifications for processing. Failure to comply with this principle is subject to the very highest fines of up to 20 million Euros or in the case of an undertaking up to 4% of annual worldwide turnover, whichever is the greater.

In particular:

- The bar for valid consents has been raised much higher under GDPR. Consents must be fully unbundled from other terms and conditions and will not be valid unless freely given, specific, informed and unambiguous (Articles 4(11) and 6(1)(a)). Consent also attracts additional baggage for controllers in the form of extra rights for data subjects (the right to be forgotten and the right to data portability) relative to some of the other legal justifications. Consent must be as easy to withdraw consent as it is to give – data subjects have the right to withdraw consent at any time – and unless the controller has another legal justification for processing any processing based on consent alone would need to cease once consent is withdrawn.
- To compound the challenge for controllers, in addition to a hardening of the requirements for valid consent, GDPR has also narrowed the legal justification allowing data controllers to process in their legitimate interests. This justification also appears in the Directive though the interpretation of the concept in the current regime has varied significantly among the different Member States with some such as the UK and Ireland taking a very broad view of the justification and others such as Germany taking a much more restrictive interpretation. GDPR has followed a more Germanic approach, narrowing the circumstances in which processing will be considered to be necessary for the purposes of the legitimate interests of the controller or a third party. In particular, the

ground can no longer be relied upon by public authorities. Where it is relied upon, controllers will need to specify what the legitimate interests are in information notices and will need to consider and document why they consider that their legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subjects, in particular where children's data is concerned.

The good news is that the justification allowing processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject to enter into a contract is preserved in GDPR, though continues to be narrowly drafted. Processing which is not necessary to the performance of a contract will not be covered. The less good news for controllers relying on this justification is that it comes with additional burdens under GDPR, including the right to data portability and the right to be forgotten (unless the controller is able to rely on another justification).

Other justifications include where processing is necessary for compliance with a legal obligation; where processing is necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent; where processing is necessary for performance of a task carried out in the public interest in the exercise of official authority vested in the controller. These broadly mirror justifications in the current Directive.

Processing for new purposes

It is often the case that organisations will want to process data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data was first collected. This is potentially in conflict with the core principle of purpose limitation and to ensure that the rights of data subjects are protected, GDPR sets out a series of considerations that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are a fresh consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Processing of special categories of personal data

As is the case in the Directive, GDPR sets a higher bar to justify the processing of special categories of personal data. These are defined to include "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." (Article 9(1)) Processing of these data are prohibited unless one or more specified grounds are met which are broadly similar to the grounds set out in the Directive.

Processing of special categories of personal data is only permitted (Article 9(2)):

- with the explicit consent of the data subject
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- in limited circumstances by certain not-for-profit bodies
- where processing relates to the personal data which are manifestly made public by the data subject

- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

The justifications and conditions for processing special categories of data is one area where Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Processing of personal data relating to criminal convictions and offences

GDPR largely mirrors the requirements of the Directive in relation to criminal conviction and offences data. This data may only be processed under official authority or when authorized by Union or Member State law (Article 10) which means this is another area where legal requirements and practice is likely to diverge among the different Member States.

Practical Implications

1. Controllers will need to ensure that they have one or more legal justifications to process personal data for each purpose. Practically this will require comprehensive data mapping to ensure that all personal data within the extended enterprise (ie including data processed by third parties as well as data within the organisation) has a legal justification to be processed.

2. Consideration will need to be given as to which are the most appropriate justifications for different purposes and personal data, given that some justifications attract additional regulatory burdens.

3. The common practice of justifying processing with generic consents will need to cease when GDPR comes into force. Consent comes with many additional requirements under GDPR and as such is likely to be a justification of last resort where no other justifications are available.

4. Where controllers propose to process legacy data for new purposes, they will need to be able to demonstrate compliance with the purpose limitation principle. To do that, controllers should document decisions made concerning new processing, taking into account the criteria set out in GDPR and bearing in mind that technical measures such as encryption or psuedonymisation of data will generally make it easier to prove that new purposes are compatible with the purposes for which personal data were originally collected.

G. TRANSFERS

International transfers and particularly those to the US have regularly made front page headline news over the last 12 months with the successful torpedoing of the EU/US Safe Harbor regime by Europe's highest court. Organisations will be relieved to hear that for the most part GDPR will not make any material changes to the current rules for transfers of personal data cross-border, largely reflecting the regime under the Directive. That said, in contrast to the current regime where sanctions for breaching transfer restrictions are limited, failure to comply with GDPR's transfer requirements attract the highest category of fines of up to 20 million Euros or in the case of undertakings up to 4% of annual worldwide turnover.

Transfers of personal data to third countries outside the EU are only permitted where the conditions laid down in GDPR are met. (Article 44)

Transfers to third countries, territories or specified sectors or an international organisation which the Commission has decided ensures an adequate level of protection do not require any specific authorisation. (Article 45(1)) The adequacy decisions made under the current Directive shall remain in force under GDPR until amended or repealed (Article 45(9)); so for the time being transfers to any of the following countries are permitted: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faero Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguary and New Zealand.

The well-publicised gap for transfers from the EU to US following the ruling that Safe Harbor is invalid will, it is hoped, be filled with the new EU/US Privacy Shield.

Transfers are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards include amongst other things binding corporate rules which now enjoy their own Article 47 under GDPR and standard contractual clauses. Again, decisions on adequacy made under the Directive will generally be valid under GDPR until amended, replaced or repealed.

Two new mechanics are introduced by GDPR to justify international transfers (Article 46(2)(e) and (f)): controllers or processors may also rely on an approved code of conduct pursuant to Article 40 or an approved certification mechanism pursuant to Article 42 together in each case with binding and enforceable commitments in the third country to apply these safeguards including as regards data subjects' rights. GDPR also removes the need to notify and in some Member States seek prior approval of model clauses from supervisory authorities.

GDPR includes a list of derogations similar to those included in the Directive permitting transfers where:

(a) explicit informed consent has been obtained
(b) the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
(d) the transfer is necessary for important reasons of public interest
(e) the transfer is necessary for the establishment, exercise or defence of legal claims
(f) the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
(g) the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanic is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48)are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; otherwise transfer in response to such requests where there is no other legal basis for transfer will breach GDPR's restrictions.

Practical Implications

1. Given the continued focus of the media and regulators on international transfer and the increased sanctions to be introduced by GDPR, all controllers and processors will need to carefully diligence current data flows to establish what types of data is being shared with which organisations in which jurisdictions.

2. Current transfer mechanics will need to be reviewed to assess compliance with GDPR and, where necessary, remedial steps implemented before GDPR comes into force.

3. For intra-group transfers, consider binding corporate rules which not only provide a good basis for transfers but also help demonstrate broader compliance with GDPR helping to comply with the principle of accountability.

H. DATA BREACH NOTIFICATION

One of the most profound changes to be introduced by GDPR is a European wide requirement to notify data breaches to supervisory authorities and affected individuals.

In the US, data breach notification laws are now in force in 47 States and the hefty penalties for failing to notify have fundamentally changed the way US organisations investigate and respond to data incidents. Not notifying has become a high risk option.

In contrast, Europe currently has no universally applicable law requiring notification of breaches. In the majority of Member States there is either no general obligation to notify or minimal sanctions for failing to do so; for many organisations not notifying and thereby avoiding the often damaging media fall-out is still common practice in Europe. That is set to change fundamentally when GDPR comes into force.

GDPR requires "the controller without undue delay, and where feasible, not later than 72 hours after having become aware of it, [to] notify the … breach to the supervisory authority" (Article 33(1)). When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals the controller is also required to notify the affected individuals "without undue delay" (Article 34). Processors are required to notify the controller without undue delay having become aware of the breach (Article 33(2)).

The notification to the regulator must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's DPO or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Although the obligation to notify is conditional on awareness, burying your head in the sand is not an option as controllers are required to implement appropriate technical and organisational measures together with a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing (Article 32). Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits by the supervisory authority.

Failing to comply with the articles relating to security and data breach notification attract fines of up to 10 million Euros or 2% of annual worldwide turnover, potentially for both the controller and the processor. As data breach often leads to investigations by supervisory authorities and often uncovers other areas of non-compliance, it is quite possible that fines of up to 20 million Euros or 4% of annual worldwide turnover will also be triggered.

Practical implications

1. Notification will become the norm: Sweeping breaches under the carpet will become a very high risk option under GDPR. Organisations that are found to have deliberately not notified can expect the highest fines and lasting damage to corporate and individual reputations. Notifying and building data breach infrastructure to enable prompt, compliant notification will be a necessity under GDPR.

2. A coordinated approach, including technology, breach response policy and training and wider staff training. Data breaches are increasingly a business as usual event. Lost or stolen devices; emails sent to incorrect addresses in error and the continuing rise of cybercrime means that for many organisations, data breaches are a daily occurrence. To deal with the volume of breaches, organisation's need a combination of technology, breach response procedures and staff training.

a. Technology requirements: these will vary for each organisation but will typically include a combination of firewalls, log recording, data loss prevention, malware detection and similar applications. There are an increasingly sophisticated array of applications that learn what "normal" looks like for a particular corporate network to be able to spot unusual events more effectively. The state of the art continues to change rapidly as organisations try to keep pace with sophisticated hackers. Regular privacy impact assessments and upgrades of technology will be required.
b. Breach response procedures: to gain the greatest protection from technology, investment is required in dealing with

red flags when they are raised by internal detection systems or notified from external sources. Effective breach response requires a combination of skill sets including IT, PR and legal. Develop a plan and test it; regularly.
c. Staff training: the weak link in security is frequently people rather than technology. Regular staff training is essential to raise awareness of the importance of good security practices, current threats and who to call if a breach is suspected. It is also important to avoid a blame culture that may deter staff from reporting breaches.

3. Consider privilege and confidentiality as part of your plan. Make sure that forensic reports are protected by privilege wherever possible to avoid compounding the losses arising from a breach. Avoid the temptation to fire off emails when a breach is suspected; pick up the phone. Don't speculate on what might have happened; stick to the facts. Bear in mind that you may be dealing with insider threat – such as a rogue employee – so keep any investigation on a strictly need to know basis and always consider using external investigators if there is any possibility of an inside attack.

4. Appoint your external advisors today if you haven't done so already. When a major incident occurs, precious time can be wasted identifying and then retaining external support teams when you are up against a 72 hour notification deadline. Lawyers, forensics and PR advisors should ideally be contracted well before they are needed for a live incident. Find out more about DLA Piper's breach response credentials and team.

5. Insurance: many insurers are now offering cyber insurance. However, there is a lack of standardisation in coverage offered. Limits are often too small for the likely exposure. Conditions are often inappropriate such as a requirement for the insured to have fully complied with all applicable laws and its own internal policies which will rarely be the case. That said, it is usually possible to negotiate better coverage with carriers in what continues to be a soft insurance market. Now is a good time to check the terms of policies and work with your legal team and brokers to ensure that you have the best possible coverage. You should clarify with brokers and underwriters what amounts to a notifiable incident to insurers under your policies as again there is no common standard and failing to notify when required may invalidate cover. You should also ensure that your insurance policies will cover the costs of your preferred external advisors as many policies will only cover advice from panel advisors.

6. Develop standard notification procedures: Perhaps the greatest challenge facing organisations and regulators is the sheer volume of data breach and the lack of standards or guidance as to how breaches should be notified and at what point they become notifiable. In the absence of guidance organisation's will need to make an informed decision as to how to develop internal operations for the detection, categorisation, investigation, containment and reporting of data breaches. Similarly, supervisory authorities will need to develop standard approaches and standard categorisations of incidents to ensure that limited resources are focussed on the most serious incidents first.

I. MORE RIGHTS FOR INDIVIDUALS

GDPR builds on the rights enjoyed by individuals under the current Directive, enhancing existing rights and introducing a new right to data portability. These rights are backed up with provisions making it easier to claim damages for compensation and for consumer groups to enforce rights on behalf of consumers.

Transparency

One of the core building blocks of GDPR's enhanced rights for individuals is the requirement for greater transparency. Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data is obtained:

- the identity and contact details of the controller
- the Data Protection Officer's contact details (if there is one)
- both the purpose for which data will be processed and the legal basis for processing including if relevant the legitimate interests for processing
- the recipients or categories of recipients of the personal data
- details of international transfers
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this

- the existence of rights of the data subject including the right to access, rectify, require erasure (the "right to be forgotten"), restrict processing, object to processing and data portability; where applicable the right to withdraw consent, and the right to complain to supervisory authorities
- the consequences of failing to provide data necessary to enter into a contract
- the existence of any automated decision making and profiling and the consequences for the data subject.
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Slightly different transparency requirements apply (Article 14) where information have not been obtained from the data subject.

Subject access rights (Article 15)

These broadly follow the existing regime set out in the Directive though some additional information must be disclosed and there is no longer a right for controllers to charge a fee, with some narrow exceptions. Information requested by data subjects must be provided within one month as a default with a limited right for the controller to extend this period for up to three months.

Right to rectify (Article 16)

Data subjects continue to enjoy a right to require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten')(Article 17)

This forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right to be forgotten now has its own Article in GDPR. However, the right is not absolute; it only arises in quite a narrow set of circumstances notably where the controller has no legal ground for processing the information. As demonstrated in the Google Spain decision itself, requiring a search engine to remove search results does not mean the underlying content controlled by third party websites will necessarily be removed. In many cases the controllers of those third party websites may have entirely legitimate grounds to continue to process that information, albeit that the information is less likely to be found if links are removed from search engine results.

The practical impact of this decision has been a huge number of requests made to search engines for search results to be removed raising concerns that the right is being used to remove information that it is in the public interest to be accessible.

Right to restriction of processing (Article 18)

Data subjects enjoys a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data is no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller and whether these override those of the data subject are contested.

Right to data portability (Article 20)

This is an entirely new right in GDPR and has no equivalent in the current Directive. Where the processing of personal data is justified either on the basis that the data subject has given their consent to processing or where processing is necessary for the performance of a contract, or where the processing is carried out be automated means, then the data subject has the right to receive or have transmitted to another controller all personal data concerning them in a structured, commonly used and machine-readable format.

The right is a good example of the regulatory downsides of relying on consent or performance of a contract to justify processing – they come with various baggage under GDPR relative to other justifications for processing.

Where the right is likely to arise controllers will need to develop procedures to facilitate the collection and transfer of personal data when requested to do so by data subjects.

Right to object (Article 21)

The Directive's right to object to the processing of personal data for direct marketing purposes at any time is retained.

In addition, data subjects have the right to object to processing which is legitimized on the grounds either of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject or that the processing is for the establishment, exercise or defence of legal claims.

The right not to be subject to automated decision taking, including profiling (Article 22)

This right expands the existing Directive right not to be subject to automated decision making. GDPR expressly refers to profiling as an example of automated decision making. Automated decision making and profiling "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" are only permitted where

(a) necessary for entering into or performing a contract
(b) authorized by EU or Member State law, or
(c) the data subject has given their explicit (ie opt-in) consent.

The scope of this right is potentially extremely broad and may throw into question legitimate profiling for example to detect fraud and cybercrime. It also presents challenges for the online advertising industry and website operators who will need to revisit consenting mechanics to justify online profiling for behavioral advertising. This is an area where further guidance is needed on how Article 22 will be applied to specific types of profiling.

Practical implications

1. Controllers will need to review and update current fair collection notices to ensure compliance with the expanded information requirements. Much more granular notices will be required using plain and concise language.

2. Consideration should be given to which legal justifications for processing are most appropriate for different purposes, given that some such as consent and processing for performance of a contract come with additional regulatory burden in the form of enhanced rights for individuals.

3. For some controllers with extensive personal data held on consumers, it is likely that significant investment in customer preference centers will be required on the one hand to address enhanced transparency and choice requirements and on the other hand to automate compliance with data subject rights.

4. Existing data subject access procedures should be reviewed to ensure compliance with the additional requirements of GDPR.

5. Policies and procedures will need to be written and tested to ensure that controllers are able to comply with data subjects’ rights within the time limits set by GDPR. In some cases, such as where data portability engages, significant investments may be required.

J. DATA PROTECTION OFFICERS

GDPR introduces a significant new governance burden for those organisations which are caught by the new requirement to appoint a DPO. Although this is already a requirement for most controllers in Germany under current data protection laws, it is an entirely new requirement (and cost) for many organisations.

The following organisations must appoint a data protection officer (DPO) (Article 37):

- public authorities
- controllers or processors whose core activities consist of processing operations which by virtue of their nature, scope or purposes require regular and systemic monitoring of data subjects on a large scale
- controllers or processors whose core activities consist of processing sensitive personal data on a large scale.

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices though perhaps in recognition of the current shortage of experienced data protection professionals, it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "properly and in a timely manner in all issues which relate to the protection of personal data." (Article 38(1)) The role is therefore a sizeable responsibility for larger controllers and processors.

The DPO must directly report to the highest management level, must not be told what to do in the exercise of their tasks and must not be dismissed or penalized for performing their tasks. (Article 38(3))

The specific tasks of the DPO are set out in GDPR including (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws
- to monitor compliance with law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- to advise and monitor data protection impact assessments
- to cooperate and act as point of contact with the supervisory authority

Practical implications

1. Organisations will need to assess whether or not they fall within one or more of the categories where a DPO is mandated. Public authorities will be caught (with some narrow exceptions) as will many social media, search and other tech firms who monitor online consumer behavior to serve targeting advertising. Many b2c businesses which regularly monitor online activity of their customers and website visitors will also be caught.

2. There is currently a shortage of expert data protection officers as outside of Germany this is a new requirement for most organisations. Organisations will therefore need to decide whether to appoint an internal DPO with a view to training them up over the next couple of years or use one of the external DPO service providers several of which have been established to fill this gap in the market. Organisations might consider a combination of internal and external DPO resources as given the size of the task it may not be realistic for just one person to do it.

K. ACCOUNTABILITY AND GOVERNANCE

Accountability is a recurring theme of GDPR. Data governance is no longer just a case of doing the right thing; organisations need to be able to prove that they have done the right thing to regulators, to data subjects and potentially to shareholders and the media often years after a decision was taken.

GDPR requires each controller to demonstrate compliance with the data protection principles (Article 5(2)). This general principle manifests itself in specific enhanced governance obligations which include:

- ***Keeping a detailed record of processing operations*** (Article 30)
  The requirement in current data protection laws to notify the national data protection authority about data processing operations is abolished and replaced by a more general obligation on the controller to keep extensive internal records of their data protection activities. The level of detail required is far more granular compared to many existing Member State notification requirements. There is some relief granted to organisations employing fewer than 250 people though the exemption is very narrowly drafted.
- ***Performing data protection impact assessment for high risk processing*** (Article 35)

A data protection impact assessment will become a mandatory pre-requisite before processing personal data for processing which is likely to result in a high risk to the rights and freedoms of individuals. Specific examples are set out of high risk processing requiring impact assessments including: automated processing including profiling that produce legal effects or similarly significantly affect individuals; processing of sensitive personal data; and systematic monitoring of publicly accessible areas on a large scale. DPOs, where in place, have to be consulted. Where the impact assessment indicates high risks in the absence of measures to be taken by the controller to mitigate the risk, the supervisory authority must also be consulted (Article 36) and may second guess the measures proposed by the controller and has the power to require the controller to impose different or additional measures (Article 58).

- ***Designating a data protection officer*** (Article 37) See Data Protection Officers
- ***Notifying and keeping a comprehensive record of data breaches*** (Articles 33 and 34) See Data Breach Notification
- ***Implementing data protection by design and by default*** (Article 25)
  GDPR introduces the concepts of "data protection by design and by default". "Data protection by design" requires taking data protection risks into account throughout the process of designing a new process, product or service, rather than treating it as an afterthought. This means assessing carefully and implementing appropriate technical and organisational measures and procedures from the outset to ensure that processing complies with GDPR and protects the rights of the data subjects.
  "Data protection by default" requires ensuring mechanisms are in place within the organisation to ensure that, by default, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and proessed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose.

Practical implications

1. Data mapping: every controller and processor will need to carry out an extensive data audit across the organization and supply chains, record this information in accordance with the requirements of Article 30 and have governance in place to ensure that the information is kept up-to-date. The data mapping exercise will also be crucial to be able to determine compliance with GDPR's other obligations so this exercise should be commenced as soon as possible.

2. Gap analysis: Once the data mapping exercise is complete, each organization will need to assess its current level of compliance with the requirements of GDPR. Gaps will need to be identified and remedial actions prioritized and implemented.

3. Governance and policy for data protection impact assessments: the data mapping exercise should identify high risk processing. Data protection impact assessments will need to be completed and documented for each of these (frequently these will include third party suppliers) and any remedial actions identified implemented. Supervisory authorities may need to be consulted. A procedure will need to be put in place to standardize future data protection impact assessments and to keep existing impact assessments regularly updated where there is a change in the risk of processing.

4. Data protection by design and by default: in part these obligations will be addressed through implementing remedial steps identified by the gap analysis and in data protection impact assessments. However, to ensure that data protection by design and by default is delivered, extensive staff and supplier engagement and training will also be required to raise awareness of the importance of data protection and to change behaviors.

L. DEROGATIONS

European data protection laws today are in many cases substantively very different among Member States. This is partly due to the ambiguities in the Directive being interpreted and implemented differently, and partly due to the Directive permitting Member States to implement different or additional rules in some areas. As GDPR will become law without the need for any secondary implementing laws, there will be a greater degree of harmonisation relative to the current regime. However, GDPR preserves the right for Member States to introduce different laws in many important

areas and as a result we are likely to continue to see a patchwork of different data protection laws among Member States, for certain types of processing.

Each Member State is permitted to restrict the rights of individuals and transparency obligations (Article 23) by legislation when the restriction "respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard one of the following:

(a) national security
(b) defence
(c) public security
(d) the prevention, investigation, detection or prosecution of breaches of ethics for regulated professions, or crime, or the execution of criminal penalties
(e) other important objectives of general public interest of the EU or a Member State, in particular economic or financial interests
(f) the protection of judicial independence and judicial proceedings
(g) a monitoring, inspection or regulatory function connected with national security, defence, public security, crime prevention, other public interest or breach of ethics
(h) the protection of the data subject or the rights and freedoms of others
(i) the enforcement of civil law claims

To be a valid restriction for the purposes of GDPR, any legislative restriction must contain specific provisions setting out:

(a) the purposes of processing
(b) the categories of personal data
(c) the scope of the restrictions
(d) the safeguards to prevent abuse or unlawful access or transfer
(e) the controllers who may rely on the restriction
(f) the permitted retention periods
(g) the risks to the rights and freedoms of data subjects
(h) the right of data subjects to be informed about the restriction, unless prejudicial to the purpose of the restriction

In addition to these permitted restrictions, Chapter IX of GDPR sets out various specific processing activities which include additional derogations, exemptions and powers for Member States to impose additional requirements. These include:

- Processing and freedom of expression and information (Article 85)
- Processing and public access to official documents (Article 86)
- Processing of national identification numbers (Article 87)
- Processing in the context of employment (Article 88)
- Safeguards and derogations to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89)
- Obligations of secrecy (Article 90)
- Existing data protection rules of churches and religious associations (Article 91)

These special cases also appear in the Directive, though in some cases have been amended or varied in GDPR.

Practical implications

1. Controllers and processors will first need to determine which Member States' laws apply to their processing activities and whether processing will be undertaken within any specific processing activities which may be subject to additional restrictions.

2. These Member State laws will then need to be checked to determine what additional requirements engage. Changes in law will need to be monitored and any implications for processing activities addressed.

3. Derogations will pose a challenge to multi-national organisations seeking to implement standard European-wide solutions to address compliance with GDPR; these will need to be sufficiently flexible to allow for exceptions where different rules engage in one or more Member State.

M. CROSS-BORDER ENFORCEMENT

The ideal of a one-stop-shop ensuring that controllers present in multiple Member States would only have to answer to their lead home regulator failed to make it into the final draft. GDPR includes a complex, bureaucratic procedure allowing multiple 'concerned' authorities to input into the decision making process.

The starting point for enforcement of GDPR is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority". (Article 56(1))

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities and there are powers for a supervisory authorities in another Member State to enforce where infringements occur on its territory or substantially affects data subjects only in its territory. (Article 56(2))

In situations where multiple supervisory authorities are involved in an investigation or enforcement process there is a cooperation procedure (Article 60) involving a lengthy decision making process and a right to refer to the consistency mechanism (Articles 63 - 65) if a decision cannot be reached, ultimately with the European Data Protection Board having the power to take a binding decision.

There is an urgency procedure (Article 66) for exceptional circumstances which permits a supervisory authority to adopt provisional measures on an interim basis where necessary to protect the rights and freedoms of data subjects.

Practical implications

1. Controllers and processors will need to determine which Member States' supervisory authorities have jurisdiction over their processing activities; which is the lead authority and which other supervisory authorities may have jurisdiction.

2. An important aspect of managing compliance risk is to try to stay on the right side of your regulator by engaging positively with any guidance published and taking up opportunities such as training and attending seminars.

KEY CONTACTS

Prof. Patrick Van Eecke
Partner
T +32 2 500 1630
patrick.van.eecke@dlapiper.com

DATA PROTECTION AND PRIVACY GROUP KEY CONTACTS

Americas

Jim Halpert
Partner & Chair of US Data Protection and Privacy Group
T +1 202 799 4441
jim.halpert@dlapiper.com

Jennifer Kashatus
Partner, Data Protection, Privacy and Security
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

Europe, Middle East and Africa

Andrew Dyson
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +44 (0)113 369 2403
andrew.dyson@dlapiper.com

Prof. Patrick Van Eecke
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +32 2 500 1630
patrick.van.eecke@dlapiper.com

Carol Umhoefer
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +33 1 40 15 24 34
carol.umhoefer@dlapiper.com

Thomas Jansen
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +49 89 2323 72 110
thomas.jansen@dlapiper.com

Diego Ramos
Partner
T +349 17901658
diego.ramos@dlapiper.com

Richard van Schaik
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +31 20 541 9828
richard.vanschaik@dlapiper.com

Asia Pacific

Peter Jones
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +61292868356
peter.jones@dlapiper.com

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

EDITORS

Kate Lucente
Associate and Co-Editor, Data Protection Laws of World Handbook
T +1 813 222 5927
kate.lucente@dlapiper.com

James Clark
Associate and Co-Editor, Data Protection Laws of the World Handbook
T +44 113 369 2461
james.clark@dlapiper.com

ANGOLA

Last modified 27 January 2016

LAW IN ANGOLA

Data Protection Law (Law no. 22/11of 17 June) and Electronic Communications and Information Society Services Law (Law no. 23/11, of 20 June 2011).

DEFINITIONS

Definition of personal data

The Data Protection Law defines personal data as any given information, regardless of its nature, including images and sounds related to a specific or identifiable individual.

An identifiable person is deemed to be an individual that may be directly or indirectly identified, notably, by reference to her/his identification number or to the combination of specific elements of her/his physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The Data Protection Law defines sensitive personal data as the personal data related to:

- philosophical or politic beliefs
- political affiliations or trade union membership
- religion
- private life
- racial or ethnic origin
- health or sex life (including genetic data).

NATIONAL DATA PROTECTION AUTHORITY

Agência de Proteção de Dados (APD). Although the Data Protection Law provides for the creation of the APD, such a body has not yet in practice been created.

REGISTRATION

In general terms, depending on the type of personal data and on the purposes of the processing either:

- prior notification, or
- prior authorisation from the APDs is required (please note that in case of authorisation depends on compliance with specific legal conditions).

The APD may exempt certain processing from the notification requirement. In general terms, notification and authorisation requests should include the following information:

- the name and address of the controller and of its representative (if applicable)
- the purposes of the processing
- a description of the data subject categories and the personal data related to those categories
- the recipients or under which categories of recipient to whom the personal data may be communicated and respective conditions
- details of any third party entities responsible for the processing
- the possible combinations of personal data
- the duration of personal data retention
- the process for a data subject to execute further rights
- any predicted transfers of personal data to third countries
- a general description (which will allow the APD to assess the suitability of the measures adopted to ensure the processing security).

DATA PROTECTION OFFICERS

There is no obligation to appoint data protection officers.

COLLECTION & PROCESSING

In general terms, personal data collection and processing of personal data is subject to express and prior consent from the data subject and prior notification to the APD. However, data subject consent is not required in certain circumstances provided by law.

With respect to sensitive data processing, collection and processing is only allowed where there is a legal provision allowing such processing or prior authorization from the APD is obtained (please note that the authorization may only be granted in specific cases provided by law). If the sensitive personal data processing results from a legal provision, the same shall be notified to APD.

There are specific rules applicable to the processing of personal data relating to:

- sensitive data on health and sexual life
- illicit activities, crimes and administrative offenses
- solvency and credit data
- video surveillance and other electronic means of control
- advertising by email
- advertising by electronic means (direct marketing)
- call recording.

Specific rules for the processing of personal data within the public sector also apply.

The data subject shall be provided with:

- the identity and address of the controller
- the purposes of the processing and of the creation of a file for such purposes

- the recipients or categories of personal data recipients
- the conditions under which the right of access, rectification, deletion, opposition and updating may be exercised, and
- the consequences of the collection of personal data without consent of the data subject.

TRANSFER

International transfers of personal data to countries with an adequate level of protection require prior notification to the APD. An adequate level of protection is understood as a level of protection equal to the Angolan Data Protection Law. APD decides which countries ensure an adequate level of protection by issuing an opinion to this respect.

International transfers of personal data to countries which do not ensure an adequate level of protection are subject to prior authorization from the APD which will only be granted in case specific requirements are fulfilled. In case of transfers between the companies of the same group, the requirement of an adequate level of protection may be reached through the adoption of harmonized and mandatory internal rules on data protection and privacy.

Please note however, that the communication of personal data to a recipient, a third party or a subcontracted entity is subject to specific legal conditions and requirements.

SECURITY

The data controller must implement appropriate technical and organizational measures and to adopt adequate security levels in order to protect personal data against accidental or unlawful total or partial destruction, accidental loss, total or partial alteration, unauthorized disclosure or access (in particular where the processing involves the transmission of data over a network) and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Specific security measures shall be adopted regarding certain type of personal data and purposes (notably, sensitive data, call recording and video surveillance).

BREACH NOTIFICATION

There is no mandatory breach notification under the Data Protection Law.

However, pursuant to the Electronic Communications and Information Society Services Law, companies offering electronic communications services accessible to the public shall, without undue delay, notify the APD and the Electronic Communications Authority, *Instituto Angolano das Comunicações*, (INACOM) of any breach of security committed with intent or recklessly that leads to destruction, loss, partial or total modification or non-authorized access to personal data transmitted, stored, retained or by any way processed under the offer of electronic communications services.

Companies offering electronic communications services accessible to the public shall also keep an accurate register of data breaches, indicating the concrete facts and consequences of each breach and the measures put in place to repair or prevent the breach.

ENFORCEMENT

Data Protection

As mentioned above, the competent authority for the enforcement of Data Protection Law is the APD. However, considering that the APD is not yet created, the level of enforcement is not significant at this stage.

Electronic Communications

INACOM regulates, inspects and verifies compliance with the Electronic Communications and Information Security Law, and applies the penalties related to violations of it. Although, unlike the APD, the INACOM exists, the level of enforcement is still not significant yet.

ELECTRONIC MARKETING

Sending of electronic communications for the purposes of advertising is generally subject to the prior express consent of its recipient ('opt-in') and to prior notification to APD.

The processing of personal data for this purposes may be conducted without data subject consent in specific circumstances, notably:

- when the advertising is addressed to the data subject as representative, employee of a corporate person and
- when the advertising communications are sent to an individual with whom the supplier of a product or a service has already concluded transactions provided the opportunity to refuse was expressly provided to the customer at the time of the transaction and this does not involve an additional cost. In this case, the data subject has the right to oppose to his personal data processing for advertising/direct marketing purposes.

ONLINE PRIVACY

The Electronic Communications and Information Security Law establishes the right for all Citizens to enjoy protection against abuse or violations of their rights through the Internet or by other electronics means, such as:

- the right to confidentiality of communications and to privacy and non-disclosure of their data
- the right to security of their information by improvement of quality, reliability and integrity of the information systems
- the right to security on the Internet, specifically for minors
- the right not to receive spam
- the right to protection and safeguarding to their consumer rights and as users of networks or electronic communications services.

In view of the above it is in general not allowed to store any kind of personal data without prior consent of the user. This does not prevent technical storage or access for the sole purpose of carrying out the transmission of a communication over an e-communication network or if strictly necessary in order for the provider of an information society service to provide a service expressly requested by the subscriber/user.

Traffic data

The processing of traffic data is allowed when required for billing and payment purposes, but processing is only permitted until the end of the period during which the bill may lawfully be challenged or payment pursued. Traffic data must be eliminated or made anonymous when no longer needed for the transmission of the communication.

The storing of specific information and the access to such information is only allowed on the condition that the subscriber/user has provided his or her prior consent. The consent must be based on accurate, clear and comprehensive information, namely about the type of data processed, the purposes and duration of the processing and the availability of data to third parties in order to provide value added services.

Electronic communication operators may also store traffic data only to the extent required and the time necessary to market electronic communications services or provide value added services. Prior express consent is required and such

consent may be withdrawn at any time.

Processing should be limited to those employees in charge of:

- billing or traffic management
- customer inquiries
- fraud detection
- marketing of electronic communications
- services accessible to the public
- the provision of value added services

Notwithstanding the above, electronic communication operators should keep in an autonomous file all traffic data and localization data exclusively for the purpose of:

- investigation
- detection or
- prosecution of criminal offences on Information and Communication Technologies (ICT).

Location data

The processing of Location Data is only allowed if the data is made anonymous or to the extent and for the duration necessary for the provision of value added services, provided prior express consent is obtained. In this case prior complete and accurate information must be provided on the type of data being processed, as well as the purposes and duration of the processing and the possibility of disclosure to third parties for the provision of value added services.

Electronic communication operators must ensure the possibility to withdraw consent at any time, or temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication. This shall be provided by using simple means, which are free of charge to the user. The processing should be limited to those employees in charge of electronic communications services accessible to the public.

KEY CONTACTS

VCA – Law Firm
www.vca-angola.com

Vera Meireles Rodrigues
Associate
T +244 926 61 25 25
vm.rodrigues@vca-angola.com

Carmina Cardoso
Of Counsel
T +244 926 61 25 25
c.cardoso@vca-angola.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

ARGENTINA

Last modified 24 January 2015

LAW IN ARGENTINA

Section 43 of the Federal Constitution grants citizens expeditious judicial action to gain access to information about them contained in public and private databases and to demand its amendment, updating, confidentiality, or suppression if it is incorrect.

Personal Data Protection Law Number 25,326 (the 'PDPL'), enacted in October 2000, provides much broader protection of personal data closely following Spain's data protection law. On 30 June 2003, the European Commission recognised that Argentina provides an 'adequate' level of protection of personal data, in line with the Data Protection Directive (95/46/EC).

DEFINITIONS

Definition of personal data

Personal information or data means *'any type of information related to identified or identifiable individuals or legal entities'*.

Definition of sensitive personal data

Sensitive information or data means *'personal information revealing racial or ethnic origin, political views, religious beliefs, philosophical or moral stands, union affiliations or any information referring to health or sexual life'*.

NATIONAL DATA PROTECTION AUTHORITY

Argentine Personal Data Protection Agency – in Spanish *Dirección Nacional de Protección de Datos Personales* (DNPDP)

Sarmiento 1118 – 5th Floor
Autonomous City of Buenos Aires
(C1041AAX) Argentina
T +54 11 4383 8512

http://www.jus.gov.ar/datos-personales.aspx

The DNPDP has enforcement power.

REGISTRATION

Any public or private database formed for the purpose of providing reports, any private database which is not formed

exclusively for personal use, and any database formed for the purpose of transferring personal data must be registered with the DNPDP. The registration must include, at least, the following information:

- name and address of the data collector
- characteristics and purpose of the database
- nature of the data included in the database
- collection and update methods
- individuals or entities to which the data may be transferred
- methods for linking the recorded information
- methods used to ensure data security, including a detail of the people with access to information processing
- time during which the data will be stored, and
- conditions under which third parties can gain access to data related to them and the procedures performed to correct or update the data.

DATA PROTECTION OFFICERS

There is no requirement in Argentina for organizations to appoint a data protection officer.

However, a 'Head of Data Security' (*Responsible de Seguridad*) must be appointed by data controllers to which 'medium' or 'high' security requirements apply. Its duties are exclusively related to ensuring compliance with database security measures.

COLLECTION & PROCESSING

In general, data controllers may only collect and process personal data with the data subject's consent. Consent is *not required* if:

- the data is collected from a publicly accessible database, in the exercise of government duties, or as a result of a legal obligation
- the database is limited to certain basic information, such as name, ID, tax ID, job, birthdate and address
- the personal data derives from a scientific or professional contractual relationship and is used only in such context, or
- the information is provided by financial institutions, provided that they were required to do so by a court, the Central Bank or a tax authority.

When collecting personal data, the data collector shall expressly and clearly inform data subjects of:

- the purpose for which the data is being collected
- who may receive the data
- the existence of a database, the identity of the data collector and its mailing address
- the consequences of providing the data, of refusing to do so or of providing inaccurate information, and

- the data subject's access, rectification and suppression rights.

In addition, data contained in databases must be truthful, adequate, pertinent, and not excessive, be used exclusively for the purpose for which it was legally obtained and be deleted on completion of that purpose. Incomplete or partially or totally false data must be immediately amended or suppressed.

No person may be required to disclose sensitive personal data. Sensitive personal data may only be collected and processed in cases of public interest, as determined by law. Anonymised sensitive personal data may be collected for statistical or scientific purposes, so long as the data subjects are no longer identifiable.

Data related to criminal history or background may only be collected by public authorities.

TRANSFER

The European Commission recognised Argentina as providing an adequate level of protection for personal data transferred from the European Community (Commission Decision C (2003) 1731 of 30 June 2003).

Personal data may only be transferred out of Argentina in compliance with legitimate interests of the transferring and receiving parties, and generally requires the prior consent of the data subject, which may be later revoked.

Consent to the transfer of personal data is not required when:

- the collection of the data did not require consent
- the transfer is made between government agencies in the exercise of their respective duties
- the data relates to health issues, and is used for emergencies, epidemiologic studies or other public health purposes, provided that the identity of the subject is protected, or
- the data have been de-identified such that they may no longer be linked with the corresponding subjects.

The transferee is subject to the same obligations as the transferor, and both parties are jointly and severally liable for any breach of data protection obligations.

Personal data may not be transferred to other countries or international institutions that do not provide an adequate level of protection, unless in cases of judicial or intelligence international cooperation, where Argentina has signed specific treaties with the relevant countries covering this issue, or in case of bank transfers or health issues (provided that the requirements set out above are complied with).

The adequate level of protection requirement may also be met by the parties including in the relevant agreement, data protection provisions similar to those contained in PDPL.

SECURITY

The data collector must take all technical and organisational measures necessary to ensure the security and confidentiality of the personal data, so as to avoid its alteration, loss, or unauthorised access or treatment. Such measures must permit the data collector to detect intentional and unintentional breaches of information, whether the risks arise from human action or the technical means used. It is prohibited to record personal data in databases which do not meet requirements of technical integrity and safety.

The level of security that must be provided varies in relation to the sensitivity of the personal data. Regulations distinguish between three possible levels of data security, based on the nature of the data stored in the database, and provide for minimum security requirements for each category.

BREACH NOTIFICATION

There are no requirements in the PDPL to report data security breaches or losses to the DNPDP or to data subjects. Nevertheless, all data incidents must be recorded by the data controller in a 'Security Incidents Ledger'. The DNPDP is entitled to request access to the Security Incidents Ledger when conducting an inspection. Notification may be necessary to mitigate potential violations in the event that the DNPDP starts an investigation and detects a security failure, which constitutes a violation of the data security obligations included in the PDPL.

ENFORCEMENT

The DNPDP is responsible for the enforcement of the data protection regime. Either acting ex officio or upon a complaint from a data subject, the National Ombudsman or consumer associations, the DNPDP is entitled to start an investigation when it suspects that the PDPL has been infringed. Administrative sanctions include warnings, suspension of the right to maintain a database, the imposition of monetary fines, ranging from AR$1,000 to AR$100,000 (approximately US$117 to US$11,700 as of January 2015), or the cancellation of the database.

In addition, data subjects may separately recover damages for violations of their data protection rights. The PDPL also modified the Argentine Criminal Code to include personal data crimes, such as knowingly inserting false information in a database, knowingly providing false information from a database, illegally accessing a restricted database, or revealing information contained in a database that the offender was in charge of keeping confidential. Criminal violations are subject to prison terms ranging from one month up to three years, which may be increased by 50% if any person suffers damage as a result of the crime.

ELECTRONIC MARKETING

The PDPL will apply to most digital marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the PDPL). In all cases, the data subjects are entitled to exercise their access, amendment and deletion rights as provided in the PDPL.

In particular, the DNPDP's Disposition No. 4/2009 sets forth that:

- all promotional messages shall include the language from the PDPL's Section 27:3 and the third paragraph of Section 27 of Decree No. 1558/01 – which set forth a data subject's right to request suppression of their personal information from marketing databases
- all marketing emails not previously requested or consented to by the data subject shall include as their subject the single word *Publicidad* (promotional), and
- senders of promotional messages shall ensure that all mechanisms needed to honour the data subject's requests are in place.

On August 5, 2014, Law No. 26,951 was published in the Official Gazzette, creating the Argentine National Do Not Call Registry. The purpose of such registry is to protect telephone service users ('Users') from abuses by companies using such means to advertise, offer, sell or give non-requested goods and services ('Advertising Companies'). Users may opt to be included in the Registry for free. Advertising Companies, which will be regarded as data collectors under the PDPL and subject to their obligations, will not be allowed to call any registered User, and will need to, on a monthly basis, verify any updates of such list. The penalties for breaches and other enforcement regulations will be those provided in the PDPL. The application authority will be the DNPDP. The law must be implemented by a Decree, which should have be issued by November 3, 2014; however, as of January 6, 2014 the Decree has not yet been issued.

ONLINE PRIVACY

Argentina has not enacted specific legislation governing online privacy, nor has the PDPL issued regulations on this point.

Particularly with regard to automatic data collection programs, the current interpretation of most scholars is that information collected by 'cookies' or similar programs does not qualify as 'personal data' because such information

corresponds to a device and not to the user him or herself.

KEY CONTACTS

Cordova Francos Gorbea D'Aiello Jofre ABOGADOS
www.cfgd.com.ar/

Sebastián Córdova-Moyano
Founding Partner
T +54 11 4311 3571
scordova@cfgd.com.ar

Felipe Oviedo Roscoe
Senior Associate
T +54 11 4311 3571
foviedo@cfgd.com.ar

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

AUSTRALIA

Last modified 24 March 2015

LAW IN AUSTRALIA

Data privacy/protection in Australia is currently made up of a mix of Federal and State/Territory legislation. The Federal Privacy Act 1988 (Cth) (Privacy Act) and its Australian Privacy Principles (APPs) apply to private sector entities with an annual turnover of at least A$3 million and all Commonwealth Government and Australian Capital Territory Government agencies.

The Privacy Act was last amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which came in to force on 12 March 2014. The amendments significantly strengthened the powers of the Privacy Commissioner to conduct investigations (including own motion investigations), ensure compliance with the amended Privacy Act and, for the first time, introduced fines for a serious breach or repeated breaches of the APPs.

Australian States and Territories (except for Western Australia and South Australia) each have their own data protection legislation applying to State Government agencies (and private businesses' interaction with them). These acts are:

- Information Privacy Act 2014 (Australian Capital Territory)
- Information Act 2002 (Northern Territory)
- Privacy and Personal Information Protection Act 1998 (New South Wales)
- Information Privacy Act 2009 (Queensland)
- Personal Information Protection Act 2004 (Tasmania), and
- Privacy and Data Protection Act 2014 (Victoria).

There is also various other State and Federal legislation that relates to data protection. For example, the Telecommunications Act 1997 (Cth), the National Health Act 1953 (Cth), the Health Records and Information Privacy Act 2002 (NSW), the Health Records Act 2001 (Vic) and the Workplace Surveillance Act 2005 (NSW) all impact privacy/data protection for specific types of data or for specific activities. Our focus here, however, is on the application of the Privacy Act to private sector entities.

Private sector entities are referred to as 'organisations'. Under the Privacy Act/the APPs, an organisation can be an:

- individual
- body corporate
- partnership
- other unincorporated association, or
- a trust.

DEFINITIONS

Definition of personal data

Personal Data (which is referred to as 'personal information' in Australia) means 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 material form or not.

Definition of sensitive personal data

Sensitive Personal Data (which is referred to as 'sensitive information' in Australia) means information or an opinion about:

- 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
- criminal record that is also personal information
- health information about an individual
- genetic information about an individual that is not otherwise health information
- biometric information that is to be used for the purpose of automated biometric identification or verification, or
- biometric templates.

NATIONAL DATA PROTECTION AUTHORITY

The Privacy Commissioner under the Office of the Australian Information Commissioner ('Privacy Commissioner') is the national data protection regulator responsible for overseeing compliance with the Privacy Act. Its website is currently http://www.oaic.gov.au/.

The Australian Government has indicated that the Office of the Australian Information Commissioner will be dismantled by 2015, with the Office of the Privacy Commissioner to become a separate regulator solely charged with enforcing the Privacy Act.

REGISTRATION

Australia does not maintain a register of controllers or of processing activities. There is no requirement under the current data protection regime (ie the Privacy Act) for an organisation to notify/report to the Office of the Privacy Commissioner on the processing of personal information.

DATA PROTECTION OFFICERS

There is no requirement for organisations to appoint a data protection officer, but it is good and usual practice under the current law and guidance has been issued by the Privacy Commissioner strongly recommending it.

COLLECTION & PROCESSING

An organisation must not collect personal information unless the information is reasonably necessary for one or more of its business functions or activities.

Under the Privacy Act organisations must also take steps, as are reasonable in the circumstances, to ensure that the personal information that the organisation collects is accurate, up-to-date and correct.

At or before the time personal information is collected, or as soon as practicable afterwards, an organisation must take reasonable steps to make an individual aware of:

- its identity and how to contact it
- why it is collecting (or how it will use the) information about them
- to whom it might give the personal information
- any law requiring the collection of personal information
- the main consequences (if any) for the individual if all or part of the information is not provided
- the fact that the organisation's privacy policy contains information about how the individual may access and seek correction of their personal information, how they may make a complaint about a breach of the APPs and how the organisation will deal with such complaint
- whether the organisation is likely to disclose their personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located.

Organisations usually comply with these notificaitons requirements by including the above information in a privacy policy and requiring individuals to accept that privacy policy prior to collecting their personal information.

One of the biggest issues in practice in respect of collection and compliance with the Privacy Act for organisations is the failure to appreciate that the obligations with respect to mandatory notification outlined above also apply to any personal information they collect from/via a third party. That is, a separate and independant obligation to notify the mandatory matters arises on the receipt of personal information from a third party, as though the organization had collected such personal information directly from the individual. In contrast to Europe, Australian privacy law does not distinguish between a 'data processor' and a 'data controller'.

An organisation must not use or disclose personal information about an individual unless one or more of the following applies:

- the personal information was collected for the primary purpose of such disclosure or a secondary purpose related to (and, in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the organisation to use or disclose the information for that secondary purpose
- the individual consents
- the information is not sensitive information and disclosure is for direct marketing and it is impracticable to seek the individual's consent and (among other things) the individual is told that they can opt out of receiving marketing from the organisation
- a 'permitted general situation' or 'permitted health situation' exists; for example, the entity has reason to suspect that unlawful activity relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public
- it is required or authorised by law or on behalf of an enforcement agency.

In the case of use and disclosure for the purpose of direct marketing, organisations are required to also ensure that:

- each direct marketing communication provides a simple means by which the individual can opt-out
- the individual has not previously requested to opt-out of receiving direct marketing communications.

Where 'sensitive information' is processed there are additional protections under the Privacy Act which generally provide

that an organisation is not allowed to collect sensitive information from an individual unless certain limited requirements are met, including one or more of the following:

- the individual has consented to the collection and the collection of the sensitive information is reasonably necessary for one or more of the entity's functions or activities
- collection is required or authorised by law or a court/tribunal order
- a 'permitted general situation' or 'permitted health situation' exists; for example the information is required to establish or defend a legal or equitable claim or he/she is a serious treat to the life or health of the individual or the public
- the entity is an enforcement body and the collection is reasonably necessary for that entity's functions or activities
- the entity is a non-profit organisation and the information relates to the activities of the organisation and solely to the members of the organisation (or to individuals who have regular contact with the organisation relating to its activities).

An organisation must, on request by an individual, give that individual access to the personal information (and the ability to correct inaccurate, out of date or irrelevant information) that is held about the individual unless particular circumstances apply which allow the organisation to limit the extent to which access is given (and to which correction is performed). These include emergency situations, specified business imperatives and law enforcement or other public interests.

Organisations must also provide individuals with the option of not identifying themselves, or of using a pseudonym, when dealing with that organisation unless it is impractical to do so or the organisation is required (or authorised) by law to deal with identified individuals.

TRANSFER

Unless certain limited exemptions under the Privacy Act apply, personal information may only be disclosed to an organisation outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the personal information. The disclosing/transferring entity will generally remain liable for any act(s) done or omissions by that overseas recipient that would, if done by the disclosing organization in Australia, constitute a breach of the APPs. However, this provision will not apply where:

- the organisation reasonably believes that the recipient of the information is subject to a law or binding scheme which effectively provides for a level of protection that is at least substantially similar to the Privacy Act, including as to access to mechanisms by the individual to take action to enforce the protections of that law or binding scheme. There can be no reliance on contractual provisions requiring the overseas entity to comply with the APPs to avoid ongoing liability (although it is a step towards ensuring compliance with the 'reasonable steps' requirement)
- the individual consents to the transfer However, under the Privacy Act the organisation must, prior to receiving consent, expressly inform the individual that if he or she consents to the overseas disclosure of the information the organisation will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs
- a 'permitted general situation' applies, or
- the disclosure is required or authorised by law or a court/tribunal order.

SECURITY

An organisation must have appropriate security measures in place (ie 'take reasonable steps') to protect any personal

information it retains from misuse and loss and from unauthorised access, modification or disclosure. The Privacy Commissioner has issued a 32 page detailed guidance document on what it considers to be "reasonable steps" in the context of security of personal information, which we recommend be reviewed and implemented. An organisation must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the purpose(s) for which it was collected.

BREACH NOTIFICATION

An organisation that breaches the Privacy Act is currently under no legal obligation (and it is not generally current practice) to report that breach to the affected individual(s) or the OAIC. However, the OAIC has issued a guidance on data breach notification which recommends that if there is a real risk of serious harm as a result of a data breach, the affected individuals and the OAIC should be notified.

ENFORCEMENT

The Privacy Commissioner is responsible for the enforcement of the Privacy Act and will investigate an act or practice if the act or practice may be an interference with the privacy of an individual and a complaint about the act or practice has been made.

The Privacy Commissioner may also investigate any 'interferences with the privacy of an individual' (ie any breaches of the APPs) on its own initiative (ie where no complaint has been made) and the same remedies as below are available.

After investigating a complaint, the Privacy Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the organisation rectify its conduct or that the organisation redress any loss or damage suffered by the complainant. Furthermore, fines of up to A$340,000 for an individual and A$1.7 million for corporations may be requested by the Privacy Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals.

ELECTRONIC MARKETING

The sending of electronic marketing (which is referred to as ‘commercial electronic messages’ in Australia) is regulated under *SPAM Act 2003* (Cth) ('SPAM Act') and enforced by the Australian Communications and Media Authority.

Under the SPAM Act a commercial electronic message must not be sent without the prior 'opt-in' consent of the recipient. In addition, each electronic message (which the recipient has consented to receive) must contain a functional unsubscribe facility to enable the recipient to opt-out from receiving future electronic marketing.

A failure to comply with the SPAM Act (including unsubscribing a recipient that uses the unsubscribe facility) may have costly consequences, with repeat offenders facing penalties of up to A$1.7 million per day.

ONLINE PRIVACY

There are no laws or regulations in Australia specifically relating to online privacy, beyond the application of the Privacy Act and State and Territory privacy laws relating to online / e-privacy, the collection of location and traffic data, or the use of cookies (or any similar technologies). If the cookies or other similar technologies collect personal information of a user the organisation must comply with the Privacy Act in respect of collection, use, disclosure and storage of such personal information. App developers must also ensure that the collection of customers' personal information complies with the Privacy Act and the Privacy Commissioner has released detailed guidance on this.

KEY CONTACTS

Peter Jones
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +61292868356
peter.jones@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

AUSTRIA

Last modified 26 January 2016

LAW IN AUSTRIA

Austria implemented the EU Data Protection Directive 95/46/EC with the Data Protection Act, Federal Law Gazette part I No. 165/1999 as amended ('Act').

DEFINITIONS

Definition of personal data

Personal data is defined as information relating to an identified or identifiable subject (including also legal entities).

Definition of sensitive personal data

Sensitive personal data refers to data relating to racial or ethnic origin, political opinions, trade union membership, religious or philosophical belief, health or sex life of a natural person.

NATIONAL DATA PROTECTION AUTHORITY

Austrian Data Protection Authority (as of January 1, 2014, *Datenschutzbehörde* previously the Data Protection Commission *Datenschutzkommission*).

REGISTRATION

Unless an exemption applies, data controllers who process personal data by automatic means must notify the Data Protection Authority ('DPA'), who keep a register of all data applications. The Data Protection Register is accessible by the public. Changes to the data application will require the notification to be amended.

An exemption applies to so called standard applications, which are defined by decree of the Federal Chancellor.

The notification shall *inter alia* include the following information (as outlined in the DPA standard notification form):

- the title and purpose(s) of the data application;
- the controller's contact details and if relevant the controller's representatives' contact details;
- the categories of personal data processed;
- whether sensitive data is processed;
- the recipients of the data (only C2C transfers);

- the legitimate authority for the data application;
- a description of security measures; and
- in cases where an approval by the DPA for the foreign data transfer is required, the reference of the respective order of the DPA.

DATA PROTECTION OFFICERS

There is no legal requirement in Austria for organisations to appoint a data protection officer. There is currently a draft amendment pending in the parliamentary proceedings which would provide the possibility to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers may collect and process personal data if they have legitimate authority and in addition any of the following conditions are met:

- the data subject consents, such consent can be revoked at any time
- the processing is necessary to enable the controller to fulfil an explicit legal authorisation or obligation
- the processing is necessary to protect the vital interests of the data subject
- the processing is necessary to enable the controller or third parties to protect a legitimate interest, except where such interest is overridden by the interests of the data subject, such as:
    - the processing is necessary to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract
    - the processing is necessary to perform a task in the public interest
    - the processing is necessary to exercise official authority
    - the processing is necessary to protect the vital interests of a third party, or
    - the processing is necessary for the establishment, exercise or defence of legal claims of the controller before a public authority

Where sensitive personal data is processed, a different, exhaustive list of specific conditions applies. With regard to sensitive data, the legitimate interest in confidentiality will not be infringed in the following circumstances:

- where the data was clearly made public by the data subject
- where the data is used only in indirectly personal form
- where the use of the data is authorised or required by law and in the public interest
- where the data is used by state authorities for inter authority assistance
- where the data relates exclusively to the exercise of a public function of the data subject, revocation being possible any time
- where the data subject has given explicit consent to the use of the data

- where processing or disclosure is necessary to safeguard the vital interests of the data subject, and consent cannot be obtained in due time
- where the use of the data is necessary to safeguard the vital interests of a third party
- where the use of the data is necessary for the enforcement, exercise or defence of legal claims of the data controller before the authorities, provided such data has been lawfully collected
- where the data is used only for private purposes, for statistical or research purposes, or for the purpose of informing or interviewing the data subject
- where the use of the data is necessary for compliance with labour or employment law
- where the use of the data is required for medical prevention, medical diagnostics, health care or treatment, or for the administration of medical services, and the data is only used by medical staff or other persons who are subject to an obligation of secrecy, or
- where data regarding political or ideological opinions of natural persons is used by non profit organisations, with political, philosophical, religious or trade union objectives, within the legitimate scope of their activities, and such data relates to members, supporters, or other persons who have on a regular basis expressed their interest in the objectives of the relevant organisation.

Whichever of the above conditions is relied upon, the controller must first provide the data subject with certain information, unless an exemption applies. The notification shall at least include information on the identity of the controller and the purposes of the processing.

The data controller should also inform the data subject of other aspects necessary to ensure that the processing is fair, such as whether or not it is obligatory to respond and the right to object to the processing.

TRANSFER

A transfer of personal data is only lawful, if:

1. the data originates from a lawful data application
2. the recipient can show a legitimate authority to receive the data, and
3. the interests of the data subjects are preserved

A transfer to recipients outside the EU/European Economic Area requires the prior approval of the DPA, unless:

- the recipient resides in a country, which by decree of the Federal Chancellor provides for "adequate protection." Following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C362/14), the USA can no longer be considered a country with an adequate protection, even in respect to companies which adhere to the US/EU Safe Harbor principles, which was also explicitly confirmed by the DPA. Unless another exemption listed here would apply, data transfers to the USA are now generally subject to approval.
- the data subject has without any doubt consented to the transfer
- a contract between the controller and the data subject or a third party, that has been concluded clearly in the interest of the data subject, cannot be fulfilled except by the trans-border transmission of data

- the data has been published legitimately in Austria
- data is transferred or committed that is only indirectly personal to the recipient
- the trans-border transfer is authorised by regulations that are equivalent to a statute in the Austrian legal system and are immediately applicable
- the data is for private purposes
- the transfer is necessary for the establishment, exercise or defence of legal claims before a foreign authority and the data was collected legitimately
- the transfer is expressly named in a standard application, or
- the transfer is made from a data application that is exempted from registration.

The DPA shall grant its approval if, in the specific case, adequate protection can be evidenced. Such safeguards may *inter alia* result from contractual clauses, eg by standard contractual clauses approved by the European Commission, or via an organisation's Binding Corporate Rules. In respect to data transfers to the USA, in spite of the reasoning of the ECJ in the *Schrems* case, the DPA has confirmed that, for the time being, the approval on the basis of the EC standard contractual clauses or the BCR is still possible.

SECURITY

Data controllers and processors must implement the appropriate technical and organisational measures, depending on the technological state of the art and the cost incurred in execution, to protect personal data against accidental or intentional destruction or loss, unauthorised disclosure or access and against all other unlawful forms of processing.

The Act thereby lists particular measures, such as a regulation of the rights of access to data and the right to operate on data.

BREACH NOTIFICATION

Since the beginning of 2010, the Act has required a data controller to notify the data subjects in an appropriate way, if it realises that the data in its data application has been systematically or in a material way unlawfully used, unless the potential damage of the data subjects is negligible or the notification would require unreasonable expense.

ENFORCEMENT

Anybody can raise a complaint with the DPA. The DPA is authorised to investigate data applications in any case of reasonable suspicion. It has the power to request clarification from the data controller and inspect documentation.

A violation of a data subject's right to secrecy, rectification or deletion of data must be brought before the competent civil court.

Failure to comply with the Act may be sanctioned by the competent administrative authority with fines up to EUR 25,000.

ELECTRONIC MARKETING

The Act does not specifically address (electronic) marketing, while the use of personal data for marketing purposes clearly falls within the remit of the Act. It is arguable that the processing of personal data within the scope of the business is permissible for marketing purposes. However, it is argued that the consent of the data subjects is required.

Electronic marketing is also regulated by the Austrian Telecommunications Act (*Telekommunikationsgesetz* 2003, 'TKG'). Pursuant to the TKG the sending of electronic messages without prior consent of the recipient is unlawful, if the sending is for direct marketing purposes and to more than 50 recipients. No consent is required if the data has been obtained in the course of the sale of goods or provision of services, occurs for the same or similar goods or services, the recipient is able to decline easily and with no costs for the use of his or her personal data and the recipient has not previously declared, by requesting to be entered on to the relevant list (maintained by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)), that he or she does not want to be contacted.

ONLINE PRIVACY

Online privacy is specifically regulated by the TKG.

Traffic Data

Traffic Data held by communications services providers ('CSPs') must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained for purposes of invoicing the services. In such a case, if the invoice has been paid and no appeal has been lodged with the CSP within three months the Traffic Data must be erased or anonymised.

Location Data

Location Data may only be processed for value added services and with consent of the user. Even in case of consent, the user must be able to prohibit the processing by simple means, for free of charge and for a certain time period.

Cookie Compliance

The relevant section of the TKG stipulates that a user must give informed consent for the storage of personal data, which includes a cookie. The user has to be aware of the fact that consent for the storage or processing of personal data is given, as well as the details of the data to be stored or processed, and has to agree actively. Therefore obtaining consent via some form of pop up or click through agreement seems advisable. Consent by way of browser settings, or a pre-selected check-box etc. is probably not sufficient in this respect.

If for technical reasons the short term storage of content data is necessary, such data must be deleted immediately thereafter.

KEY CONTACTS

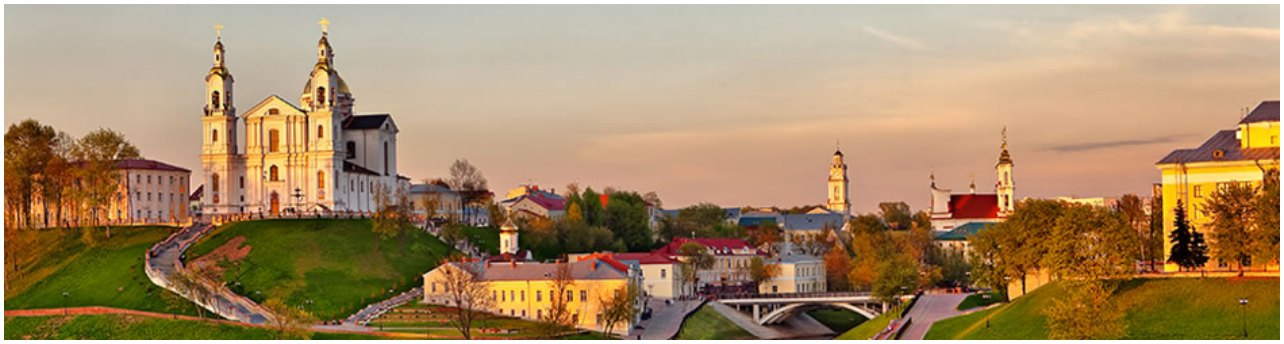
Sabine Fehringer
Partner
T +43 1 531 78 1460
sabine.fehringer@dlapiper.com

Stefan Panic
Associate
T +43 531 78 1034
stefan.panic@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

BELARUS



Last modified 25 January 2016

LAW IN BELARUS

The main legal acts regulating personal data protection in Belarus are the Law on Information, Informatisation and Information Protection of 10 November 2008 No. 455 Z (hereinafter referred to as the 'Information Protection Law') and the Law on Population Register of 21 July 2008 No. 418 Z (hereinafter referred to as the 'Population Register Law').

The acts implemented within the framework of the Eurasian Economic Union should also be taken into consideration, eg the Protocol on Informational Communication Technologies and Informational Interaction within the Eurasian Economic Union, Annex 3 to the Treaty on the Eurasian Economic Union of 29 May 2014.

DEFINITIONS

Definition of personal data

According to the Information Protection Law personal data are basic and additional personal data of an individual which are subject to the admission to the population registry, as well as other data which allow identifying such an individual. The basic personal data are defined by the Population Register Law as a closed list of the data including:

- name
- surname
- birth date
- citizenship
- address details.

The additional personal data are also defined by the Population Register Law as a closed list of the data including eg data on:

- a spouse
- children
- relatives
- tax obligation
- education etc.

Belarus law does not define the notion 'other data which allow identifying individual'.

Definition of sensitive personal data

There is no concept of sensitive personal data under Belarus law currently.

NATIONAL DATA PROTECTION AUTHORITY

There are two main authorities occupied primarily with overseeing data protection: Operational and Analytical Centre under the President of the Republic of Belarus (hereinafter referred to as the 'Centre') and the Ministry of Communications and Informatisation of the Republic of Belarus (hereinafter referred to as the 'Ministry').

REGISTRATION

Belarus law does not require the registration of information systems (eg databases) that contain personal data or to register as a processor of personal data for private owned information systems. For state information systems Belarus law requires registration with the Ministry regardless whether any personal data are processed in it. Such registration can be carried out for private owned information systems voluntarily. According to the Information Protection Law state information systems are information systems created and (or) acquired at republican or local budget costs, state off budget funds costs, as well as at state legal entities costs.

DATA PROTECTION OFFICERS

State bodies and legal entities which are carrying out personal data processing shall establish special departments or select employees who are going to be responsible for the information protection in such a state body or a legal entity. If technical methods of information protection are used, eg encryption, there shall be a special department on technical information protection established by such state bodies and legal entities.

COLLECTION & PROCESSING

Collection and processing of personal data are subject to the following mandatory conditions:

- to be carried out only with a written consent of the individual to which the personal data belong
- to be carried out in information systems equipped with information protection systems using technical and cryptographic means of protection certified in accordance with Belarus law
- to be carried out with implementing certain legal, organisational and technical measures of personal data protection.

The legal measures may include concluding agreements with an individual whose personal data are collected and processed. Such agreements should stipulate the terms of personal data usage, as well as parties responsibility for breach of such terms.

The organisational measures may include establishing a special entrance regime to the premises where the collection and processing are carried out, and design a list of employees which can have an access to such premises and data.

The technical measures may include using cryptography and other possible measures of control over information protection to be carried out by state bodies and legal entities on condition that a special department or employees are selected for overviewing information protection in such state bodies and legal entities.

TRANSFER

According to the Information Protection Law, transfer of personal data shall be carried out with written consent of the individual to whom the personal data transferred belongs. There are no specific requirements established for transfer of personal data from Belarus to abroad.

In practise, the employers receiving the personal data of their employees carry out possible measures (legal, organisational, technical etc.) to prevent illegal distribution of personal data and comply with Information Protection Law requirements.

SECURITY

The legal entities and (or) individuals using personal data shall carry out in accordance with Belarus law appropriate legal, organisational, technical measures of information protection in order to establish personal data protection from

their illegal distribution.

BREACH NOTIFICATION

There are no requirements under Belarus law to report the personal data protection breaches either to the state authorities, or the individuals whose personal data are concerned.

Mandatory breach notification

There are no mandatory requirements under Belarus law to report the personal data protection breaches either to the state authorities, or the individuals whose personal data are concerned.

ENFORCEMENT

Enforcement of the Law on Information Protection is primarily carried out by the Ministry and the Centre. Currently Belarus law does not provide for any liability for the breach of the regulation on personal data protection. Belarus law does provide for administrative liability in the form of a fine with (or without) a confiscation of the information protection means used, if applying information protection systems and (or) using technical and cryptographic means of protection that are not certified in accordance with Belarus law. The administrative fine amounts up to 20 basic units (approx. EUR 186, as of 30 November 2015) for individuals and up to 100 basic units (EUR 1 867 as of 30 November 2015) for legal entities.

ELECTRONIC MARKETING

Electronic marketing is subject to the rules established by the Law on Advertising of 10 May 2007 No. 225 Z (hereinafter referred to as the 'Advertising Law') and the Law on Mass Media of 17 June 2008 No. 427 Z (hereinafter referred to as the 'Mass Media Law').

According to the Advertising Law names, pen names, images or expressions of the Belarusian citizens cannot be used in the advertisement without their consent. Distribution of advertisements by means of telecommunication networks eg telephone, telex, facsimile, mobile telephone communications, e mail can be carried out only with consent of a subscriber or an addressee. The advertisement distributor is obliged to stop immediately the distribution of advertising to a subscriber or an addressee who made such a demand.

Individuals and entities the rights of which have been violated in the result of manufacture and distribution of advertisement are entitled to refer to the court with the corresponding claims.

According to the Law on Mass Media distributing information messages and/or material prepared with the use of audio , video recording, motion picture photography and photograph of an individual in the mass media without his consent is allowed only when taking the measures against possible identification of this individual by third parties, as well as on condition that the constitutional freedoms and rights are not violated and such distribution is carried out to the public interest. These requirements are not applicable to the cases when the distribution is required by the court, enforcement agencies.

ONLINE PRIVACY

Belarus law does not specifically regulate on line privacy. General requirements applicable to the personal data protection shall be applicable.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kaupo Lepasepp
Partner
T +372 6 400 900
kaupo.lepasepp@sorainen.com

Mihkel Miidla
Senior Associate, Head of Technology & Data Protection
T +372 6 400 959
mihkel.miidla@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

BELGIUM

Last modified 12 January 2016

LAW IN BELGIUM

Belgium implemented the EU Data Protection Directive 95/46/EC with the Data Protection Act dated 8 December 1992 as amended in 1998 (Act). Enforcement is through the Belgian Data Protection Authority (DPA), called the Commission for the Protection of Privacy.

Belgium expressed the importance of privacy and data protection by appointing a Secretary of State (ie a member of the cabinet assigned to a Minister) responsible for privacy matters, in October 2014.

Future legislation?

A bill reviewing the current Belgian Data Protection Act has been introduced by some Members of Parliament in the Belgian Chamber of Representatives. New rules similar to the current European draft regulation would be introduced, including an information security breach notification duty, the replacement of the general notification duty by the mandatory appointment of an information security officer, and the introduction of administrative fines.

We expect that the Parliament will postpone the vote of this bill until after the official publication of the European Data Protection Regulation. In any case, the amended Act, once enacted, would serve as a transitional legal framework until superseded by the European Data Protection Regulation.

In addition, the Belgian Secretary of State responsible for privacy matters has announced that he will propose draft legislation in order give the DPA the competence to issue fines. Under current Belgian legislation, the DPA does not have the right to impose fines upon companies infringing data protection laws and must refer such companies to the courts in case the DPA wishes them to be sanctioned.

DEFINITIONS

Definition of personal data

Personal data means any information relating to an identified or identifiable natural person.

A person is considered to be an identifiable person when he or she 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.

Definition of sensitive personal data

The Act distinguishes between three categories of sensitive personal data, for which distinct rules apply:

- personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, sex

life or trade union membership

- health related personal data, and
- personal data relating to disputes which have been submitted to courts and tribunals as well as to administrative judicial bodies, regarding suspicions, prosecutions or convictions in matters of crime, administrative sanctions or security measures

NATIONAL DATA PROTECTION AUTHORITY

Commission for the Protection of Privacy, Drukpersstraat 35
1000 Brussels
T +32 (0)2 274 48 78
F +32 (0)2 274 48 35
commission@privacycommission.be
www.privacycommission.be

REGISTRATION

Unless an exemption applies, data controllers who process personal data by automatic means must notify the DPA so that their processing of personal data may be registered and made public. Changes to the processing of personal data will require the notification to be amended.

The notification shall *inter alia* include the following information (as outlined in the DPA standard notification form):

1. the purpose(s) of the processing
2. the controller's contact details and if relevant the contact details of the controller's representative
3. the types of personal data being processed
4. whether categories of sensitive personal data are processed and if so, which categories
5. the categories of recipients of the data and the guarantees which must be applied to the communication to third parties
6. the way in which data subjects will be informed of the processing and the department which data subjects may contact to use their right to access
7. the data retention terms
8. a general description of security measures, and
9. in cases where the data will be transferred outside the European Economic Area, categories of data to be transferred and for each category of data, the country of destination.

DATA PROTECTION OFFICERS

There is no legal requirement in Belgium for organisations to appoint a data protection officer. It is, however, recommended to do so.

The Act requires controllers and processors to take adequate technical and organisational security measures.

As part of this obligation the DPA has issued 'Security Reference Measures', which reflect what is to be considered as

constituting 'adequate technical and organisation security measures'. Although the Security Reference Measures are not part of the Act itself and are not legally binding, they do have an important moral value.

The Security Reference Measures recommend controllers to appoint a so called 'information security officer'. This security officer is responsible for the implementation of the personal data security policy.

COLLECTION & PROCESSING

Legal basis for processing

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject unambiguously consents
- the processing is necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract
- the processing is necessary for compliance with a legal obligation to which the controller is subject
- the processing is necessary 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 official authority vested in the controller or in a third party to whom the data are disclosed, or
- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Where sensitive personal data is processed, a different list of specific conditions applies.

Information vis-à-vis data subjects

Prior to the processing activity, the controller must provide the data subject with certain information, unless an exemption applies. The notification shall include at least information on the identity of the controller, the purposes of the processing, the existence of the right to object in the case of personal data processing for direct marketing purposes, as well as the right to access and rectification, the recipients or categories of recipients of the personal data, and whether or not it is obligatory to respond to the data controller's request to submit personal data and any possible consequences of not responding.

TRANSFER

Transfer of a data subject's personal data to non EU/European Economic Area countries is allowed if the countries provide 'adequate protection', as decided upon by the European Commission.

Data controllers may transfer personal data out of the European Economic Area to countries which are not deemed to offer adequate protection if any of the following exceptions apply:

- the data subject has unambiguously consented to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the data controller, or for the performance of tasks at the request of the data subject prior to entering into such a contract
- the transfer is necessary for the conclusion or performance of a contract with a third party in the interest of the data subject
- the transfer is necessary in order to protect the vital interests of the data subject

- the transfer is necessary in order to establish, exercise or defend a legal claim
- the transfer is necessary or legally required in order to protect an important public interest, or
- there is statutory authority for demanding data from a public register.

The DPA may allow transfers even if the above conditions are not fulfilled if the controller adduces additional safeguards with respect to the protection of the rights of the data subject. Such safeguards may *inter alia* result from contractual clauses, eg by standard contractual clauses approved by the European Commission (EU model clauses), or via an organisation's Binding Corporate Rules.

New rules on EU model clause transfers have been introduced in 2013. All data transfer agreements must formally be submitted to the DPA for scrutiny. Where the agreement is in line with the EU model clauses, the DPA will confirm compliance. Where significant derogations to the EU model clauses have been made, the DPA will assess its compliance with Belgian legislation and, if accepted, formally approve the transfer following a strict procedure including authorisation by Royal Decree.

Following the Judgment of the Court of Justice of the European Union of 6 October 2015 (C-362/14) the US-EU Safe Harbor regime is no longer regarded as a valid basis for transferring personal data from the European Economic Area to the US. In this respect, the DPA has stated to be "*particularly happy with the ruling taking into account the fact that it clearly recognizes that it is important that national supervisory authorities intervene whenever privacy disputes arise*".

SECURITY

Data controllers and processors must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The DPA issued guidelines in respect of such security measures, called the 'Security Reference Measures'. The DPA also issued a recommendation on security measures and data breaches, following several widely publicised data breaches in Belgium. The recommendation builds further on its previously issued guidelines and details specific security requirements regarding among others IT architecture and development and production environments.

The DPA also announced its intention to strengthen the legal framework for security measures. Given recent publicised data breaches in Belgium, the DPA considered it should not only have the competence to merely recommend security measures, but should also be able to legally enforce those measures.

BREACH NOTIFICATION

The Act does not provide for a general data security breach notification duty for all data controllers.

However, in its recent recommendation on security measures and data breaches, the DPA recommends that companies notify security breaches in case of 'public incidents'. Companies should document notification procedures for data security breach incidents. In case of a 'public incident', the DPA should be informed of the causes and damage within 48 hours. A public information campaign will be initiated within 24 to 48 hours after such notification. The DPA does not specify what is to be understood by a 'public incident'.

The DPA has made available a standard data breach notification form on its website, along with a manual providing guidance on how to complete the form. The form can be completed and filed electronically via the website.

ENFORCEMENT

The DPA is authorised to investigate complaints, and to act as a mediator in case of complaints. The DPA may also appoint experts, may require the provision of documents, and may require access to certain premises. In the case of

criminal actions, the DPA must notify the public prosecutor.

Failure to comply with the Act may be criminally sanctioned with imprisonment and/or fines up to EUR 600,000.

The DPA also publicly announced its intention to make enforcement its number one priority, eg by setting up a dedicated inspection task force, and conducting increased control and inspection activities on all organisations massively processing customer data for advertising purposes as well as in specific industry sectors, such as insurance and heath care.

In 2015 the DPA has put its intention into practice by taking a very popular social network to court for non-compliance with the Belgian cookie rules. In first instance, the social network has been sentenced to stop its illegal practices subject to a daily fine of EUR 200,000. The social network has, however, announced that it will appeal the decision.

Whatever the outcome may be in appeal, it is clear that Belgium is becoming one of the more assertive countries when it comes to privacy and data protection.

ELECTRONIC MARKETING

The Act applies to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to object to the processing of their personal data (ie a right to 'opt out') for direct marketing purposes.

Additionally, specific rules are set out in the Belgian e-commerce legislation (Book XII of the Code of Economic Law) regarding opt-in requirements:

- These rules apply to all 'electronic messages', ie traditional emails, text messages (Short Message Systems or SMS), etc. Other types such as instant messaging and chat may also fall within the scope of these rules depending on the specific context. This covers not only clear promotional messages, but also newsletters and similar communications. Indeed, any form of communication intended for the direct or indirect promotion of goods, services, the image of a company, organisation or person which/who exercises a commercial, industrial or workmanship activity or regulated profession falls within the scope of these rules.

- As a general principle, the prior, free, specific and informed consent of the recipient of the message must be obtained ('opt-in principle').

- Two exceptions apply to the opt-in principle. No prior, free, specific and informed consent is to be obtained if:
    - the electronic marketing message is sent to existing customers of the service provider; or
    - the electronic message is sent to legal persons (eg to a general email address such as info@company.com).

- These exceptions are subject to compliance with strict conditions. Furthermore, all electronic messages must contain a clear reference to the recipient's right to opt out, including means to exercise this right electronically.

ONLINE PRIVACY

Cookies

Article 5 (3) of the E-Privacy Directive has been implemented into Belgian Law by means of amendment of article 129 of the Belgian Electronic Communication Act.

The use and storage of cookies and similar technologies requires:

1. clear and comprehensive information, and

2. consent of the website user.

Consent is not required for cookies that are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- strictly necessary for the provision of a service requested by the user.

In February 2015 the DPA has issued a recommendation on the use of cookies with useful guidance relating to the information obligation, the consent requirement and the exemptions.

Location data

Article 123 of the Belgian Electronic Communication Act stipulates that mobile network operators may process location data of a subscriber or an end user only to the extent the location data has been anonymised or if the processing is carried out in the framework of the provision of a service regarding traffic or location data.

The processing of location data in the framework of a service regarding traffic or location data is subject to strict conditions set forth in article 123.

Processing of location data must in addition also comply with the general rules stipulated by the Data Protection Act.

Traffic data

In accordance with article 122 of the Belgian Electronic Communication Act, mobile network operators are required to delete or anonymise traffic data of their users and subscribers as soon as such data is no longer necessary for the transmission of the communication (subject to compliance with cooperation obligations with certain authorities).

Subject to compliance with specific information obligations and subject to specific restrictions, operators may process certain location data for the purposes of:

- invoicing and interconnection payments
- marketing of the operator's own electronic communication services or services with traffic or location data (subject to the subscriber's or end user's prior consent)
- fraud detection

KEY CONTACTS

Prof. Patrick Van Eecke
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +32 2 500 1630
patrick.van.eecke@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

BOSNIA AND HERZEGOVINA

Last modified 24 March 2015

LAW IN BOSNIA AND HERZEGOVINA

The Law on Protection of Personal Data ('Official Gazette of BIH', nos. 49/06, 76/11 and 89/11) ('DP Law') is the governing law regulating data protection issues in Bosnia and Herzegovina ('BiH'). The DP Law entered into force on 4 July 2006 and its current version (after amendments made in 2011) is in force from 3 October 2011.

DEFINITIONS

Defenition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person. The data subjects are natural persons whose identity can be determined or identified, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Defenition of sensitive personal data

The DP Law defines sensitive personal data as any data relating to

- racial, national or ethnic origin
- political opinion, party affiliation, or trade union affiliation
- religious, philosophical or other belief
- health
- genetic code
- sexual life
- criminal convictions, and
- biometric data.

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Agency ('DPA') is the national data protection authority in BiH. The DPA is seated in

Vilsonovo šetalište 10
Sarajevo
www.azlp.gov.ba

REGISTRATION

Each data controller (defined as a person or legal entity which processes personal data) has to provide the DPA with specific information on the database containing personal data ('Database') established and maintained by the controller.

The DPA keeps publicly available register of data controllers and Databases.

The Database's registration includes two phases:

1. the first phase represents notification of intention to establish the Database to the DPA
2. the second phase includes reporting the Database's establishment which has to be done within 14 days.

Registration of the Database is made by submitting the application in the prescribed form to the DPA.

The DPA form includes information regarding:

- data controller
  - its name, and
  - address of its registered seat, and
- the Database itself
  - processing purpose
  - legal ground for its establishment
  - identification of exact processing activities
  - types of processed data
  - categories of data subjects, and
  - transfer of data abroad etc.

If there is a subsequent change in the registered data, for example changing initial processing activities, the change needs to be reported to the DPA within 14 days from the date the change occurred.

DATA PROTECTION OFFICERS

There is no statutory obligation that the entity which processes personal data has a data protection officer. The Rules on the Manner of Keeping and Special Measures of Personal Data Technical Protection ('Official Gazette of BiH' no. 67/09) ('Rules') stipulate that a controller can have an administrator of the Database. Such administrator is a natural person authorized and responsible for managing the Database and ensuring privacy and protection of personal data processing, in particular regarding implementation of security measures, storage and protection of data.

COLLECTION & PROCESSING

Collection and processing of personal data is permissible if carried out pursuant to the data subject's consent and in compliance with the basic principles of personal data protection.

The form of the data subject's consent depends on the type of personal data collected and processed. While the collection and processing of sensitive personal data requires explicit written consent from the data subject, the consent for the collection and processing of personal data falling within a category of general personal data does not have to be in writing. However, at the request of the competent authority, the controller has to be able to prove, at any time, the existence of a data subject's consent for processing of both personal and sensitive personal data. Therefore, having a written consent for collection of any personal data is advisable. When needed, written consent has to contain minimum elements prescribed by the DP law.

Apart from the consent, there are also other conditions which must be met for the collection and processing to be regarded legitimate. These conditions are considered the basic principles of personal data protection and are applicable to each case of personal data processing. For example, processing must be done in a fair and lawful way; the type and scope of processed data must be proportionate to the respective purpose, and other principles which guarantee legitimate reasons for personal data processing.

The DP Law provides for the exception when a data subject's personal data may be processed without the data subject's consent. This is the case where the processing is necessary for the fulfilment of a data controller's statutory obligations or for preparation or realization of an agreement concluded between a data controller and a data subject

('Exceptional Cases').

TRANSFER

Under the transfer rules set out in the DP Law, processed personal data may be transferred to countries where adequate level of personal data protection is ensured. In that regard, preferential status is given to the member states of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention'), since it is considered that countries – members of the Convention ensure adequate level of personal data protection.

Personal data transfer to countries which do not provide for adequate level of personal data protection is allowed in certain cases stipulated by the DP Law, for example:

- when the data subject consented to the transfer and was made aware of possible consequences of such transfer
- when it is required for the purpose of fulfilling the contract or legal claim, or
- when it is required for the protection of public interest.

In addition, the DPA may exceptionally approve the transfer to a country that does not ensure adequate level of personal data protection if the controller in the country where the data is to be transferred can provide for sufficient guarantees in regard to the protection of privacy and fundamental rights and freedoms of the data subject.

SECURITY

The DP Law prescribes that both data controllers and, within the scope of their competencies, the processors are required:

- to take care of data security and to undertake all technical and organizational measures
- to undertake measures against unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transfer, other forms of illegal data processing, as well as measures against misuse of personal data, and
- to adopt personal data security plan ('Security Plan') which specifies technical and organizational measures for the security of personal data.

As provided by the Rules (as defined in the section 'Data Protection Officers'), the Security Plan includes the categories of processed data and the list of instruments for protection of the data to ensure confidentiality, integrity, availability, authenticity, possibility of revision and transparency of the personal data.

Moreover, the Rules prescribe that the controller is required to undertake more stringent technical and organizational measures when processing sensitive personal data. Such measures aim at enabling recognition of each authorized access to the information system, operation with the data during the controller's regular working hours and cryptographic protection of the data transmission via telecommunications systems with appropriate software and technical measures.

Manner of personal data keeping and personal data protection in automatic processing is also closely regulated by the Rules.

BREACH NOTIFICATION

The DP Law does not impose data security breach notification duty on the controller. However, the Rules do impose a duty on the Database's administrator, processor and performer to inform the controller on any attempt of unauthorized access to information system for the Database's management.

However, the regulations issued by the Communication Regulatory Agency ('RAK') should be considered. The Regulation on Carrying out the Activities of the Publicly Available Electronic Communication Networks ('Official Gazette of BiH' no. 66/12) ('Regulation A') stipulates that the operator of publicly available electronic communication networks ('Operator') is required to inform RAK about its activities, operations and other applicable information required for RAK's regulatory competences. Since RAK's Regulation on Conditions for Providing the Telecommunications Services and Relation with End Users ('Official Gazette of BiH' no. 28/13) ('Regulation B') prescribes for the Operator's obligation to undertake such methods which will protect the privacy of users and others, in a manner that will ensure the integrity and confidentiality of data, it can be concluded that the Operator is required to notify RAK of any breach of security and integrity of public telecommunication services that resulted in violation of protection of personal data or privacy of the respective services' s users.

When it comes to the notification duty towards the users, the Regulation B obliges the Operator to inform the users adequately (eg in user agreement, in its terms and conditions or in the appropriate technical way) about the possibility of privacy or telecommunication facilities violations.

ENFORCEMENT

Enforcement of the DP Law is done by the DPA. The DPA is authorized and obliged to monitor implementation of the DP Law, both *ex officio*, and upon a third party complaint. If the DPA finds that a particular person/entity processing personal data acted contrary to the data processing rules, it may request from the controller to discontinue such processing and order specific measures to be carried out without delay.

When acting upon the complaints, the DPA may also issue a decision by which it can order blocking, erasing or destroying of data, adjustment or amendment of data, temporary or permanent ban of processing, issue warning or reprimand to the controller. The decision of the DPA may not be appealed; however, a party may initiate administrative dispute before the Court of BiH.

The DPA can initiate a misdemeanour proceeding against the respective data controller before the competent court, depending on the gravity of the particular misconduct and the data controller's behaviour with respect to the same. The offences and sanctions are explicitly prescribed by the DP Law, which includes monetary fines for a controller in the amount between approximately EUR 2,550 and EUR 51,100, as well as for the controller's authorized representative in the amount between approx. EUR 100 and EUR 7,700.

Breach of personal data protection regulations represents a criminal offence of unauthorized collection of personal data by all criminal codes applicable in BiH (Criminal Code of BiH, Criminal Code of the Republic of *Srpska*, Criminal Code of the Federation of BiH and Crimes Code of *Brčko Distrikt*). Prescribed sanctions are monetary fines (in amount to be determined by the court) or imprisonment up to six (6) months (Criminal Code of BiH; Criminal Code of the Federation of BiH; Criminal Code of the *Brčko Distrikt)* or up to one (1) year (Criminal Code of the Republic of *Srpska*).

ELECTRONIC MARKETING

Although electronic marketing is not governed by the DP Law, the respective law regulates protection of personal data used in direct marketing. In that regard, the controller is not allowed to disclose personal data to a third party without the data subject's consent. However, when that is necessary for the protection of the controller's rights and interests and when it is not in contradiction with the data subject's right to the protection of personal privacy and personal life, the personal data may be used for direct marketing purposes without consent. The DPA is of the opinion that previous provision could be used only in explicit cases, when the controller is offering products or services to regular client in order to limit possible future damages for which he could be held responsible.

Under the Regulation B, the Operator is not allowed to use personal data of the users for the purposes of its business or other promotions, unless it obtained explicit consent from the users to whom such data relates.

ONLINE PRIVACY

The general data protection rules, as introduced by the DP Law, are relevant for on-line privacy as well, as there are no specific regulations that explicitly govern on-line privacy. This includes obligation to act in accordance with the basic principles of personal data protection set out in the DP Law as well as acting on the basis of the data subject's informative consent.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Mirna Milanović Lalic
Senior Associate
T +387 33 261 535
mirna.lalic@karanovic-nikolic.com

Lana Deljkic
Senior Associate
T +387 33 261 535
lana.deljkic@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

BRAZIL

Last modified 8 July 2016

LAW IN BRAZIL

Currently, Brazil does not have a single statute establishing data protection framework. There are two bills of laws, namely, No. 330/2013 and No. 5.276/2016, under analysis before Congress that, when enacted, will specifically and broadly regulate such subject matter locally.

According to the developments of both future regulations, Bill of Law No. 5.2726/16 ("Bill of Law"), dated of May 13, 2016, is likely to be enacted in the near future, since the Presidency declared it with a status of urgency under the terms of Section 64 of Brazilian Federal Constitution, thus, Bill of Law No. 330/13 should be disregarded.

In the absence of specific law, Federal Law No. 12.965/2014 ("Brazilian Internet Act"), and its recently enacted regulating Decree No. 8.771/16 ("Decree"), dated of May 11, 2016, has brought some provisions on security and processing of personal data, as should be pointed out in the following.

For instance, the Brazilian Internet Act which establishes general principles, rights and obligations for the use of the Internet, has some relevant provisions concerning the storage, use, treatment, and disclosure of data collected on-line. Also, its regulating Decree has brought first legal definition of personal data on its Section 14.

Besides the above scenario, most aspects of data privacy are still regulated by general principles and provisions on data protection and privacy in the Federal Constitution, in the Brazilian Civil Code and in laws and regulations that address particular types of relationships (e.g. Consumer Protection Code[1] and labor laws), particular sectors (eg financial institutions, health industry, telecommunications etc), and particular professional activities (eg medicine and law). Additionally, there are laws on the treatment and safeguarding of documents and information handled by governmental entities and bodies that have privacy implications.

The Federal Constitution provides that:

- the intimacy, private life, honour and image of persons are inviolable;
- the confidentiality of correspondence and electronic communication is protected; and
- everyone is ensured access to information, although the confidentiality of the source shall be safeguarded whenever necessary for the exercise of a professional activity.

Discussion of privacy and data protection legislation has increased recently and highly expected that Brazil shall enact its first data protection statute in the near future.

[1] Due to a broad interpretation established in case law, practically every internet user is considered a "consumer" for

the purposes of the consumer protection.

DEFINITIONS

Definition of personal data

Recently enacted Decree has established the definition of personal data as any “data related to identified or identifiable natural person, including identifying numbers, electronic identifiers or locational data, when these are related to a person”.

Even though Decree is related to the Internet Civil Framework, and such laws are not specifically aimed at data protection (for this purpose, Bill of Law under discussion), the above legal definition of personal data is in accordance with the current prevailing interpretations of legal scholars and the Courts on the matter. Moreover, the current text of Bill of Law reflects the above legal definition of personal data in a broader manner. Thus, the Decree currently fills a gap until the specific law is enacted.

Definition of sensitive personal data

There is no legal definition of "sensitive data" or the equivalent in due force in Brazil. However, Bill of Law defines sensitive data as “personal data on racial or ethnic origin, religious beliefs, political opinions, membership of unions or organizations of religious, philosophical or political character, data related to health or sexual preference and genetic or biometric data”.

NATIONAL DATA PROTECTION AUTHORITY

The Decree granted legal authority to the Brazilian Internet Committee (“CGI.br”) to define security standards and incident response, making the competent authority to regulate internet security procedures and turning the guidelines on the matter established by the Committee in 2015 into legally enforceable. It was also granted regulatory and oversight competence to the National Telecommunication Agency (ANATEL), the National Consumer Secretariat and the Brazilian System to Defend Competition, each within the scope of their regulatory field, to investigate and take actions, if necessary, with regards to the data protection on internet ambience.

Furthermore, Bill of Law designates the creation of a Competent Office in charge of the implementation and supervision of the Law, and of the National Counsel of Personal Data Protection and Privacy, compound by fifteen represents of relevant offices, such as CGI.br, Prosecutor’s Office and Congress.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer in the current legal scenario. However, when Bill of Law is enacted, parties holding and processing personal data will be obliged to name an individual and/or an entity to act, accordingly to the following definitions, as responsible, operator and designated.:

- Responsible - natural or legal person, public or private, who is responsible for the decisions related to the processing of personal data. Such agent will be responsible for informing the data owner about the hypothesis of data treatment, guarantee the transparency on the data treatment, and report in case of any security incident. Also, the Responsible has the burden of proof regarding the proper collection of consent from the data owner to its data treatment;
- Operator – performs the treatment based on the instructions provided by the Responsible; and
- Designated – which will receive complaints and reports from the data owners, provide information and adopt providences, receive communications of the competent agencies, guide employees on data protection practices,

among others.

COLLECTION & PROCESSING

The Brazilian Internet Act establishes that the free, informed and express consent of Internet user is required for the collection, use, storage, transfer and treatment of personal data on-line. Any such data shall be used only for the purposes that are

- justified by the collection
- not forbidden in law
- set forth in the services agreement or terms of use of Internet applications.

In other sectors, in general, there is no formal requirement to obtain prior written consent to collect personal data submitted by the subject. However, the use, treatment and protection of such data are still subject to some restrictions.

Specific statutes and case law establishes that the scope of collection, treatment and use of personal data must be restricted to the purpose for which the data was originally collected. There is also a common understanding that certain sensitive data (e.g. religion, sexual orientation, criminal background etc) should not be collected and used for any discriminatory purpose; if a company collects and uses such sensitive data it should obtain the person's consent.

In particular, the Brazilian Consumer Protection Code establishes that a consumer should be notified in writing of the opening of a consumer file, form, registry or database containing personal data regarding a consumer if the consumer did not request that it be opened. Consumers are entitled to have access to personal data and databases about themselves and to demand immediate correction whenever they find that the data or files are incorrect. Other limitations apply. For example, negative information (such as relating to debts, breach of agreements etc.) may not be retained for more than five years.

Bill of Law also set forth that personal data treatment shall only occur upon prior free, informed and unequivocal consent from its owner, observing some principles as good faith, purpose of use, necessity, quality, transparency, security, among others.

TRANSFER

Brazilian law does not expressly restrict cross border data transfer. However, some general principles may imply restrictions on the cross border transfer of personal data in certain cases (eg clinical trial data and medical records). In the absence of specific legislation, geographic transfer should be permitted upon informed consent from the parties involved.

In case Bill of Law is enacted in its current text, international transfer of data will be allowed if the country guarantees to individuals a sufficient level of protection similar to Brazilian legislation. Such protection level will be assessed by the Competent Office, concerning the general legislation of the country, type of data and possible security measures.

SECURITY

In view of applicable general principles, data processors in Brazil are required to take reasonable technical, physical and organizational measures to protect the security of personal data, but, generally, there are no specific requirements, restrictions or details on how security should be implemented.

The Brazilian Internet Act now establishes that service providers, networks and applications providers should keep access records (such as IP addresses, logins etc) confidential, in a secured and controlled environment.

Decree established guidelines on safety standards, as follows:

- Strict control on data access by defining the liability of persons who will have the possibility of access and exclusive access privileges to certain users;

- Prospective of authentication mechanisms for records access, using, for example, dual authentication systems to ensure individualization of the controller records;
- Creation of detailed inventory of access to connection records and access to applications containing the time, duration, the identity of the employee or the responsible person for the access designated by the company and the accessed file; and
- Use of solutions of records management thru techniques which ensures the inviolability of data, such as encryption or equivalent protective measures.

CGI.br shall be responsible to promote studies and recommend procedures, rules, technical and operational standards according to the specificities and the size of the connection and application providers.

If such records are not kept for a reasonable period of time, which is determined according to the nature of the business, the service provider, network or applications provider may face prosecution. The data retention period may be extended upon request of public authorities and the obligation of keeping such records cannot be assigned or transferred to third parties.

BREACH NOTIFICATION

Security breach notification is not mandatory, yet recommended as set forth by CGI.br guidelines. Furthermore, Bill of Law will establish the mandatory breach notification to the Competent Office in case of security incidents as well as immediate communication to the affected data owners in case personal security is affected or any harm may occur from such incident

Additionally, Federal Law No. 12,737/2012 (“Hacking Law”) set forth that the owner of the personal data or the breached device may – although not obligated to do so – notify public authorities in order to conduct enquiries, so as to identify and prosecute the individual responsible for the crime of hacking and/or invasion of protected device established therein.

ENFORCEMENT

The Decree granted legal authority to CGI.br, ANATEL, the National Consumer Secretariat and the Brazilian System to Defend Competition, each within the scope of their regulatory field, to investigate and take actions, if necessary, with regards to the data protection on internet matters.

Nonetheless, enforcement can occur through administrative procedures, individual civil suits or class actions, which can be initiated by the data subject, by public authorities (eg State Attorney's Office, Consumer Protection Office and the regulator for the relevant industry) or by associations that defend collective interests.

Such public authorities may impose fines and, where relevant, revoke licenses or permits. Civil damages can be significant, because infringements of privacy rights may entitle the defendant to moral damages. Most case law on privacy and data protection involves violations of consumer rights.

The Brazilian Internet Act also establishes that the infringement of privacy and/or intimacy rights on the Internet is subject to a fine of up to 10% (ten per cent) of the aggregate turnover of the economic group of the undertaking in the country. Any offices or subsidiaries of foreign companies established in Brazil are jointly liable for the payment of the fine.

It is worth mentioning the existence of habeas data, a remedy provided for in the Federal Constitution, which can be used to gain access to personal data contained in records or databases of governmental bodies or entities having a public character, and for the correction of the applicant's data contained in such records and databases.

ELECTRONIC MARKETING

There is no federal law specifically addressing electronic marketing.

On January 9, 2012, the State of Rio de Janeiro enacted State Law 6,161/2012, which provides penalties for the offering of products and services by so-called collective buying websites within territorial limits of the same State. Under this law, information on offers and promotions may be sent only to clients previously registered through the website who have expressly consented to receive such information via email.

There is also a bill currently under discussion in the Senate which intends to amend the Brazilian Consumer Protection Code to establish as an abusive practice the unsolicited offer of products and/or services through electronic means or telephone.

In spite of the lack of a specific statute, the general provisions on privacy and intimacy rights, as well as consumer protection rights still apply; thus, a sender should immediately cease sending any sort of electronic marketing if so requested by the consumer.

ONLINE PRIVACY

.

The Brazilian Internet act has several provisions concerning the storage, use, treatment and disclosure of data collected on the Internet. Also, the established rights of privacy, intimacy and consumer rights apply equally to electronic media, such as mobile devices and the Internet.

So, violations of these rights may be subject to civil enforcement. It is generally understood that the gathering and exploitation of personal data from a user through cookies without consent are contrary to the Brazilian Internet Act, and to privacy and intimacy rights, if the data subject is identifiable (ie the information is directly linked to a particular user, IP address, device or other particular identifier etc). The same rationale applies to location data, which is considered a more sensitive type of personal data.

Therefore, cookies, location data and equivalent online data collection methods are permitted if either:

- the data subject's free and informed consent is obtained, or
- it is not possible to recognize or identify the data subject (if data cannot be linked to a given subject it does not affect privacy and intimacy rights).

Finally, it is also worth mentioning that Hacking Law 12,737/2012 criminalises the installation or exploiting of software, devices and/or vulnerabilities within an electronic device in order to obtain illicit advantage. So data collectors should be cautious as to the nature and extent of the cookies and other applications operating in the data subject's system.

KEY CONTACTS

Campos Mello Advogados
www.camposmello.adv.br/

Diego Mattos Osegueda
Associado
T +55 21 2217-2046
diego.mattos@camposmello.adv.br

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

BRITISH VIRGIN ISLANDS

Last modified 24 January 2015

LAW IN BRITISH VIRGIN ISLANDS

There is currently no formal legislation regulating data protection in the British Virgin Islands (BVI) however, the BVI Government has pledged the promulgation of suitable data protection legislation, based on internationally recognised standards, to be enacted in the near future.

English Common law is persuasive (although not binding) in the BVI and accordingly, a BVI Court will recognise and subscribe to the Common law duties of confidentiality and privacy. In essence, a person's details will need to be kept confidential provided an appropriate and satisfactory exception applies. Moreover, the duty of confidentiality has been statutorily codified in various aspects of BVI legislation, in particular the Banks and Trust Companies Act, 1990 (as amended) which regulates all banking and trust/ fiduciary related activities in the BVI.

In terms of specific exceptions, limitations on the duty of confidentiality and privacy would arise in terms of appropriate anti money laundering legislation (primarily regulated by the BVI Proceeds of Criminal Conduct Act, 1997 and the Anti Money Laundering Regulations, 2008).

DEFINITIONS

Definition of personal data

No specific definition at present. Data Protection Bill to be promulgated in the near future which will contain definitions as appropriate.

Definition of sensitive personal data

No specific definition at present. Data Protection Bill to be promulgated in the near future which will contain definitions as appropriate.

NATIONAL DATA PROTECTION AUTHORITY

No specific data protection authority at present pending promulgation of data protection legislation in the near future. The Courts of the BVI would be guided by English Common law duties of confidentiality and privacy. Moreover, the Financial Services Commission (the 'Commission') regulates the fiduciary and trust business sectors, pursuant to the Banks and Trust Companies Act, 1990 (as amended).

REGISTRATION

No specific mechanisms of registration pending the promulgation of data protection legislation in the near future.

DATA PROTECTION OFFICERS

There is presently no requirement for the appointment of data protection officers in the BVI.

COLLECTION & PROCESSING

Entities, which manage and maintain personal information data will be subject to the Common law duty of confidentiality. From a fiduciary/trust perspective, licensees are under a general obligation to maintain the privacy and confidentiality of a client's personal information unless specific permission is granted for its release or dissemination to third parties. This obligation may however be limited pursuant to the requirements of appropriate anti money laundering legislation/regulations.

From a corporate perspective, the Registrar of Corporate Affairs (the 'Registrar') is able to release only limited information regarding the particulars of any registered company including the name, type of company, the date of registration/incorporation, the address of its registered office and the status of the company. Accordingly, details of shareholders and directors are not available for public inspection (unless specifically authorised and filed by the company itself). Except where assistance to law enforcement agencies to combat illicit activity is mandated or authorised, disclosure of information by government officials, professional agents, attorneys and accountants and their employees is prohibited.

TRANSFER

Transfer of data to third parties would be subject to the Common law duty of confidentiality (which may include a statutory duty (where the Common law duty of confidentiality has been codified) depending on the nature of data being transferred). A transferor would need to ensure that appropriate measures have been taken in order to obtain the necessary consents/ approvals prior to such data being disseminated.

On 1 September 2014 the Computer Misuse and Cybercrime Act, 2014 came into force which regulates and penalises the unauthorised transfer and dissemination of information stored on a computer.

The Commission is under a general obligation of confidentiality but has the power to disclose in certain circumstances, including disclosure to foreign regulators in approved jurisdictions of information necessary to enable the regulator to exercise similar functions to those exercised by the Commission. However, before doing so, the foreign regulator is required to undertake that the information will not be transmitted to any other person without the prior written consent of the commission.

SECURITY

There are no formal statutory security measures currently in place (pending the promulgation of appropriate data protection legislation in the near future), however the holder would be subject to a general obligation to ensure the technical and organisational safeguarding of such confidential information and personal data.

BREACH NOTIFICATION

There is no current mechanism or requirement in place to report data security breaches in the British Virgin Islands.

ENFORCEMENT

Presently, the Commission and the BVI Courts will be tasked with the enforcement of data protection and confidentiality related matters (insofar as applicable pending promulgation of appropriate data protection legalisation).

ELECTRONIC MARKETING

No formal electronic communications regulations or legislation currently in place however, the Telecommunications Act (No 10 of 2006) regulates the telecommunications industry in the British Virgin Islands and provides sanctions protecting the confidentially and disclosure of personal information.

ONLINE PRIVACY

No such legislation at present in the British Virgin Islands.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Alan Hughes
Senior Associate
T +1 284 494 4030
alan.hughes@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

BULGARIA

Last modified 26 January 2016

LAW IN BULGARIA

Bulgaria implemented the EU Data Protection Directive 95/46/EC with the Personal Data Protection Act (In Bulgarian: *Закон за защита на личните данни*), promulgated in the State Gazette No. 1 of 4 January 2002, as amended periodically ('Act'). The Act came into force on1 January 2002.

The Act was last amended by the State Gazette, Issue No. 15 of 15 February 2013.

DEFINITIONS

Definition of personal data

Personal data means *'any information relating to an individual who is identified or can be identified directly or indirectly by ID or by one or more specific signs'*.

Definition of sensitive personal data

Sensitive personal data means personal data:

- revealing racial or ethnic origin
- revealing political, religious or philosophical beliefs, political parties or organisations, associations with religious, philosophical, political or trade union purposes, or
- concerning health, sexual life or the human genome.

NATIONAL DATA PROTECTION AUTHORITY

The Bulgarian data protection authority (DPA) is the Personal Data Protection Commission (In Bulgarian: Комисия за защита на личните данни):

2 Professor Tsvetan Lazarov, Sofia 1592
Bulgaria

kzld@cpdp.bg
www.cpdp.bg

REGISTRATION

Unless an exemption applies, prior to initiating any personal data processing data controllers must apply for registration

with the DPA. The registration covers the data controller and the personal data registers controlled by it. Changes to the initial registration will require notification of the DPA prior to implementing such changes. The registration is free of charge.

The DPA support the following public registers:

- register of registered data controllers
- register of data controllers exempt from registration, and
- register of data controllers with refused registration.

The prior notification shall *inter alia* specify the following information (as outlined in the DPA standard notification forms):

- Application Form covering data controllers' details, such as:
  - the controller's identification details
  - the controller's location
  - whether the controller processes data for the purposes of defence, national security, public order or criminal proceedings
  - the controller's main activity
  - whether the purpose and the means of processing are determined by the controller or by the law
  - whether the data is processed by the controller or data processor, or
  - the number of data registers
- Registry Description Form covering each separate register:
  - name and full address of the register
  - the purpose(s) of the processing
  - legal ground of the processing - whether automatic or non-automatic means are used
  - the categories of data subjects
  - the categories of personal data processed, including sensitive data (if processed)
  - the recipients or categories of recipients of the personal data
  - whether a data transfer to foreign countries is required and the specific countries
  - sources for collection of the data
  - whether an explicit consent of the data subjects is available
  - level of risk assessed for the personal data processed under the register, and
  - descriptions of technical and organisational measures for data protection in accordance with the determined levels of risk and the minimum measures set forth in DPA regulation.

The last two points were introduced with regulation adopted by the DPA requiring each data controller to conduct risk assessment of the personal data registers it operates on the basis of criteria set forth by the DPA. Further, the DPA developed in its regulation minimum technical and organisational measures obligatory for the data controller and proportionate to the level of risk of its registers.

Exemptions apply in the following situations:

- data controllers operating the public register on the basis of law which is publicly accessible or accessible to those who have a legal interest

- non profit making organisations carrying out enumerated processing, and

- data controllers explicitly exempt from registration by the DPA on the basis that the processing does not endanger the rights and legal interests of data subjects. The rules and conditions for this exemption are specified in a special regulation of the DPA. In such cases the data controller should apply for and obtain the DPA's decision on the exemption of registration. However, such decision would not relieve the respective data controllers from the DPA's control under the Act.

DATA PROTECTION OFFICERS

There is no legal requirement in Bulgaria for organisations to appoint a data protection officer ('DPO'). Appointment of a DPO is currently only recommended since it helps to build and develop a focus for data protection compliance efforts. It would be a positive signal to the DPA who may investigate the company that the company takes data protection compliance seriously.

COLLECTION & PROCESSING

Any personal data must be processed in a way that is consistent with the following general principles:

- processed fairly and lawfully
- processed only for specific and legal purposes and used only for the purposes stated at the time it is collected
- adequate, relevant and not excessive for the purposes for which it is processed
- accurate, complete and where necessary kept up to date
- not kept in a personally identifiable form longer than necessary
- processed in accordance with the rights of the data subject under applicable law
- kept securely, and
- not transferred to countries that do not have adequate data protection laws unless the data exporter takes certain specific steps to ensure that the data is adequately protected.

In addition to the general principles above, data controllers may only process personal data if one of the following conditions are satisfied:

- the processing is pursuant to a statutory obligation of the data controller
- the respective person has provided his/her explicit consent
- the processing is necessary for the performance of a contract to which the data subject is a party
- the processing is necessary for the protection of the life and health of the data subject
- the processing is necessary for the controller to carry out certain duties, in the public interest or by virtue of law, or
- the processing is necessary for the purpose of legitimate interests pursued by the data controller or data recipients, provided that the interests of the data subject are protected.

Should the personal data be considered ‘sensitive’ specific processing conditions must be satisfied.

Whichever of the above conditions is relied upon, the controller must first provide the data subject with certain information, unless an exemption applies, namely:

- identification data of the controller and its representative
- the purposes for which the data will be processed
- the recipients or categories of recipients to whom the personal data may be disclosed

- whether the provision of personal data is obligatory or voluntary and the consequences if the data is not provided (applicable if the data is gathered directly from the person to whom it relates)
- the categories of personal data relating to the respective individual (applicable if the data is not gathered directly from the data subject), or
- information about the right of access to the data and the right to rectify the collected data.

The prior notification obligation is not applicable to a data controller who does not collect the data directly from the data subject and where one of the below conditions is present:

- processing is made for statistical purposes or for the purposes of historical or scientific research and the provision of the data is impossible or would involve a disproportionate effort
- recording or disclosure of data is explicitly laid down by law, or
- the individual to whom such data relates already has the required information.

TRANSFER

The transfer of personal data within the European Union ('EU') and European Economic Area ('EEA') is free and should be in compliance with the applicable Bulgarian data protection law.

The transfer of personal data outside of the EU and the EEA is permissible only on the condition that the recipient state can ensure an adequate level of personal data protection within its territory. The assessment concerning the adequacy of the level of personal data protection in the recipient state should be made by the DPA.

The DPA should not undertake an assessment where a decision of the European Commission has to be implemented whereby the European Commission has ruled that:

1. the country to which the personal data are transferred has ensured an adequate level of protection, or
2. certain appropriate contractual clauses are in place ensuring the adequate level of protection (the EU model contractual clauses).

It shall be noted that the Personal Data Protection Act does not recognise the use of binding corporate rules ('BCR') as a separate legal ground for transfers of personal data. The DPA recently had an occasion to assess (for the first time) the implementation of BCR for transfers of personal data outside Bulgaria and EU within a multinational corporate group. Since the BCRs are not recognised as a separate justification for the transfer, the DPA analysed them as (and if) evidencing appropriate safeguards undertaken by the corporate group to permit the transfer. Thus, most of the data controllers prefer to combine the BCR with EU model contract clauses and facilitate the procedure before the DPA.

Should the DPA consider that the protection level of personal data protection in the recipient state is unsatisfactory, it may prohibit the personal data transfer. Even in such a case, the DPA may authorise the transfer should the data controller provide sufficient warranties with respect to the protection of the individual's fundamental rights. In any case, the data controller should notify the DPA in advance of its intention to transfer personal data to countries outside the EU and EEA by specifying the countries of transfer, the purpose of the transfer and the categories of personal data subject to transfer.

The Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of *Schrems* (C-362/14) provided the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. However, US safe harbop certification was never recognized by the Bulgarian DPA as a separate ground for data transfers to USA. Rather, it should have always been accompanied with one of the other recognized grounds for data transfers outside EU (i.e. EU model clauses, consent, etc.). Thus, its invalidation brings limited effects under Bulgarian law, while at the same time, new enhance framework rules at EU level are widely expected.

SECURITY

Data controllers must implement appropriate technical and organisational measures to protect personal data against accidental or intentional destruction or loss, unauthorised disclosure or access, amendments or distribution and against all other unlawful forms of processing. Data controllers must implement special protection measures in cases of electronic data transfer.

The minimum level of technical and organisational measures, as well as the minimum required type of protection are determined by the DPA in accordance with the different levels of risk of the registers and further specified by the DPA in a regulation. The Act requires data protection measures to be adopted in an internal instruction issued by the data controller and to be announced in the registration application before the DPA.

BREACH NOTIFICATION

The Act does not provide for a data security breach notification duty. However, following the entering into force of Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, the notification requirements/obligations and procedures introduced therein shall be applicable for the Bulgarian DPA and data controllers as well.

ENFORCEMENT

The DPA is responsible for the enforcement of the Act. Either acting ex officio or upon a complaint from a data subject the DPA is entitled to:

1. initiate an investigation
2. provide mandatory instructions, including but not limited to ordering the database to be erased when it does not comply with the data protection regulations
3. provide a mandatory term for rectification of the breach
4. temporarily prohibit any unlawful data processing, after preliminary notification (temporary prohibition of data processing could be imposed also in case of failure by the data controller to comply with the Commission's mandatory instructions), and
5. impose administrative sanctions.

Administrative sanctions in the form of fines for violations of the Act range from BGN 10,000 to BGN 100,000 (approximately EUR 5,000 to EUR 50,000).

Data controllers are liable for any damage caused to an individual as a result of unlawful processing or by breaching the technical requirements of data protection. The data controller is also liable for any damage caused by a data processor acting on behalf of the data controller.

The DPA decisions are subject to appeal before the Bulgarian Supreme Administrative Court within 14 days of receipt and the data subject may, in the case of an infringement of his/her rights under the Act, appeal against actions and acts of the data controllers before the relevant administrative court or the Supreme Administrative Court, as the case may be, in accordance with the general rules governing jurisdiction.

The transfer or distribution of computer or system passwords which results in the illegitimate disclosure of personal data constitutes a crime under the Bulgarian Criminal Code (promulgated in the State Gazette No. 26 of 2 April 1968, as amended periodically) and the penalty for such a crime includes imprisonment for up to three years.

ELECTRONIC MARKETING

Data protection of electronic marketing falls under the general regulations of the Personal Data Protection Act which currently requires the explicit consent of the data subject for processing of his/her personal data.

There are grounds for lawful processing of personal data listed in the Personal Data Protection Act (as mentioned above) but taking into account their limited and specific scope, for the purposes of emarketing the explicit consent of the data subject is likely to be the only applicable ground. The absence of a special legal framework concerning exclusively data protection in emarketing makes the optin regime the only possible legitimate method of pursuing emarketing. In addition, the Personal Data Protection Act explicitly provides, as part of the rights of the data subjects given under law, the right to subsequently object to any data processing for the purposes of the direct marketing. This is further supported by the current regulations in other legal acts concerning specifically direct marketing activities.

The Bulgarian Ecommerce Act explicitly requires, when it comes to direct marketing to natural persons, the optin mechanic to be mandatorily applied. Moreover, after the natural person's consent is provided, the person shall always be given the opportunity to optout from the direct marketing network and refuse his/her personal data to be further processed for such purposes.

ONLINE PRIVACY

Neither the current Personal Data Protection Act, nor other legislative act in force, presents a general framework or protection regime for processing of personal data as part of any kind of online activities, including cookies and traffic and location data. Certain regulations in this regard are set forth in the Electronic Communications Act concerning specifically providers of electronic communicational services (such as telecoms) and certain categories of users' data they can keep for the purposes of criminal and other investigations but under strictly regulated circumstances and for a limited time. In the absence of other rules, the general regime for processing of personal data shall apply and the data controller shall insure lawful processing, complied with the abovementioned requirements.

KEY CONTACTS

Wolf Theiss
www.wolftheiss.com/

Anna Rizova
Partner
T +359 2 8613703
anna.rizova@wolftheiss.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

CANADA

Last modified 24 January 2015

LAW IN CANADA

In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/ criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, and remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

The summary below focuses on Canada's private sector privacy statutes:

- Personal Information Protection and Electronic Documents Act ('PIPEDA')
- Personal Information Protection Act ('PIPA Alberta')
- Personal Information Protection Act ('PIPA BC'),
- Personal Information Protection and Indentity Theft Prevention Act ('PIPITPA') (not yet in force), and
- An Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Privacy Act'),

(collectively, 'Canadian Privacy Statutes').

PIPEDA applies:

1. to consumer and employee personal information practices of organisations that are deemed to be a 'federal work, undertaking or business' (eg banks, telecommunications companies, airlines, railways, and other interprovincial undertakings)

2. to organisations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted 'substantially similar' legislation (PIPA BC, PIPA Alberta and the Quebec Privacy Act have been deemed 'substantially similar'), and

3. to inter provincial and international collection, use and disclosure of personal information.

PIPA BC, PIPA Alberta and the Quebec Privacy Act apply to both consumer and employee personal information practices of organisations within BC, Alberta and Quebec, respectively, that are not otherwise governed by PIPEDA.

DEFINITIONS

Definition of personal data

'Personal information' includes any information about an identifiable individual.

Definition of sensitive personal data

Not specifically defined.

NATIONAL DATA PROTECTION AUTHORITY

1. Office of the Privacy Commissioner of Canada ('PIPEDA')
2. Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta')
3. Office of the Information and Privacy Commissioner for British Columbia ('PIPA BC'), and
4. *Commission d'accès à l'information du Québec* ('Quebec Privacy Act')

REGISTRATION

There is no registration requirement under Canadian Privacy Statutes.

DATA PROTECTION OFFICERS

PIPEDA, PIPA Alberta, PIPA BC and PIPITPA expressly require organisations to appoint an individual responsible for compliance with the obligations under the respective statutes.

COLLECTION & PROCESSING

Canadian Privacy Statutes set out the overriding obligation that organisations only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Subject to certain limited exceptions prescribed in the Acts, consent is required for the collection, use and disclosure of personal information. Depending on the sensitivity of the personal information, consent may be opt in or opt out. Organisations must limit the collection of personal information to that which is necessary to fulfil the identified purposes and only retain such personal information for as long as necessary to fulfil the purposes for which it was collected.

Each of the Canadian Privacy Statutes have both notice and openness/transparency requirements. With respect to notice, organisations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected. With respect to openness/transparency, generally Canadian Privacy Statutes require organisations make information about their personal information practices readily available.

All Canadian Privacy Statutes contain obligations on organisations to ensure personal information in its records is accurate and complete, particularly where the information is used to make a decision about the individual to whom the information relates or if the information is likely to be disclosed to another organisation.

Each of the Canadian Privacy Statutes also provides individuals with:

1. a right of access to personal information held by an organisation, subject to limited exceptions, and
2. a right to correct inaccuracies in/update their personal information records.

Finally, organisations must have policies and practices in place that give effect to the requirements of the legislation and organisations must ensure that their employees are made aware of and trained with respect to such policies.

TRANSFER

When an organisation transfers personal information to a third party service provider (ie who acts on behalf of the transferring organisation), the transferring organisation remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation. In particular, the transferring organisation is

responsible for ensuring that the third party service provider appropriately safeguards the data, and would also be required under the notice and openness/transparency provisions to reference the use of third party service providers in and outside of Canada in their privacy policies and procedures.

With respect to the use of foreign service providers, PIPA Alberta specifically requires a transferring organisation to include the following information in its privacy policies and procedures:

- the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and
- the purposes for which the third party service provider outside Canada has been authorised to collect, use or disclose personal information for or on behalf of the organisation.

Under PIPA Alberta, specific notice must also be provided at the time of collection or transfer of the personal information and must specify:

- the way in which the individual may obtain access to written information about the organisation's policies and practices with respect to service providers outside Canada, and
- the name or position name or title of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organisation.

In addition, under the Quebec Privacy Act, an organization must take reasonable steps to ensure that personal information transferred to service providers outside Quebec will not be used for other purposes and will not be communicated to third parties without consent (except under certain exceptions prescribed in the Act). The Quebec Privacy Act also specifically provides that the organization must refuse to transfer personal information outside Quebec where it does not believe that the information will receive such protection.

SECURITY

Each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organisations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorised access, disclosure, copying, use, modification or destruction. These laws do not generally mandate specific technical requirements for the safeguarding of personal information.

BREACH NOTIFICATION

Currently, PIPA Alberta and PIPITPA are the only Canadian Privacy Statute with breach notification requirements. However, proposed amendments to PIPEDA would require notice of material breaches to be made to the Office of the Privacy Commissioner of Canada ('OPC') and, in certain circumstances, to the individuals affected.

In Alberta, an organisation having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorised access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result.

Notification to the Commissioner must be in writing and include:

- a description of the circumstances of the loss or unauthorised access or disclosure
- the date or time period during which the loss or unauthorised access or disclosure occurred
- a description of the personal information involved in the loss or unauthorised access or disclosure

- an assessment of the risk of harm to individuals as a result of the loss or unauthorised access or disclosure
- an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorised access or disclosure
- a description of any steps the organisation has taken to reduce the risk of harm to individuals
- a description of any steps the organisation has taken to notify individuals of the loss or unauthorised access or disclosure, and
- the name and contact information for a person who can answer, on behalf of the organisation, the Commissioner's questions about the loss of unauthorised access or disclosure.

Where an organisation suffers a loss of or unauthorised access to or disclosure of personal information as to which the organisation is required to provide notice to the Commissioner, the Commissioner may require the organisation to notify the individuals to whom there is a real risk of significant harm. This notification must be given directly to the individual (unless specified otherwise by the Commissioner) and include:

- a description of the circumstances of the loss or unauthorised access or disclosure
- the date on which or time period during which the loss or unauthorised access or disclosure occurred
- a description of the personal information involved in the loss or unauthorised access or disclosure
- a description of any steps the organisation has taken to reduce the risk of harm, and
- contact information for a person who can answer, on behalf of the organisation, questions about the loss or unauthorised access or disclosure.

In Manitoba, an organisation must, as soon as reasonably practicable, notify an individual if personal information about the individual that is in its custody or under its control is stolen, lost or accessed in an unauthorized manner. This requirement to notify an individual does not apply where:

- the organisation is instructed to refrain from doing so by a law enforcement agency that is investigating the theft, loss or unauthorized accessing of the personal information, or
- the organisation is satisfied that it is not reasonably possible for the personal information to be used unlawfully.

The exact form of the notice that must be provided to individuals has not yet been prescribed.

On 8 April 2014, proposed amendments to PIPEDA were introduced that, if passed, would require that organisations report to the OPC '*any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individua*l'. The proposed amendments also require organisations to notify an affected individual 'if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual'. The proposed amendments are not yet in force.

ENFORCEMENT

Privacy regulatory authorities have an obligation to investigate complaints, as well as the authority to initiate complaints.

Under PIPEDA, a complaint must be investigated by the Commissioner and a report will be prepared that includes the Commissioner's findings and recommendations. A complainant (but not the organisation subject to the complaint) may apply to the Federal Court for a review of the findings and the court has authority to, among other things, order an organisation to correct its practices and award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner resulting in an order. Organisations are required to comply with the order within a prescribed time period, or apply for judicial review. In both BC and Alberta, once an order is final, an affected individual has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the breach.

In Alberta and BC, a person that commits an offence may be subject to a fine of not more than $100,000. Offences include, among other things, collecting, using and disclosing personal information in contravention of the Act (in Alberta only), disposing of personal information to evade an access request, obstructing the commissioner, and failing to comply with an order.

Similarly, under the Quebec Privacy Act, an order must be complied with within a prescribed time period. An individual may appeal to the judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.

A failure to comply with the Quebec Privacy Act's requirements in respect of the collection, storage, communication or use of personal information is liable to a fine of up to $10,000 and, for a subsequent offence, to a fine up to $20,000. Any one who hampers an inquiry or inspection by communicating false or inaccurate information or otherwise is liable to a fine of up to $10,000 and, for a subsequent offence, to a fine of up to $20,000.

Under the PIPITPA, it is an offence to (a) willfully collect, use, or disclose personal information in contravention of the Act, (b) wilfully attempt to gain or gain access to personal information in contravention of the Act, and (c) dispose of or alter, falsify, conceal or destroy personal information or any record relating to personal information, or direct another person to do so, with an intent to evade a request for access to information or the record. A person who commits an offence is liable on summary conviction, in the case of a person other than an individual, to a fine of not more than $100,000.

ELECTRONIC MARKETING

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed above), as well as Canada's Anti-Spam Legislation ('CASL').

Under CASL it is prohibited to send, or cause or permit to be sent, a commercial electronic message (defined broadly to include text, sound, voice, or image messages aimed at encouraging participation in a commercial activity) unless the recipient has provided express or implied consent and the message complies with the prescribed content and unsubscribe requirements (subject to limited exceptions).

What constitutes both permissible express and implied consent is defined in the Act and regulations. For example, an organization may be able to rely on implied consent when there is an existing business relationship with the recipient of the message, based on:

- a purchase by the recipient within the past two years, or
- a contract between the organization and the recipient currently in existence or which expired within the past two years

CASL also prohibits the installation of a computer program on any other person's computer system, or having installed such a computer program cause any electronic messages to be sent from that computer system, without express consent, if the relevant system or sender is located in Canada. In addition, the Act contains anti phishing provisions that prohibit (without express consent) the alteration of transmission data in an electronic message such that the message is delivered to a destination other than (or in addition to) that specified by the sender.

CASL also introduced amendments to PIPEDA that restrict 'address harvesting', or the unauthorized collection of email addresses through automated means (ie using a computer program designed to generate or search for, and collect, email addresses) without consent. The use of an individual's email address collected through address harvesting also is restricted.

The 'Competition Act' was also amended to make it an offence to provide false or misleading representations in the sender information, subject matter information, or content of an electronic message.

CASL contains potentially stiff penalties, including administrative penalties of up to $1 million per violation for individuals and $10 million for corporations (subject to a due diligence defence). CASL also sets forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL ($200 for each contravention up to a maximum of $1 million each day for a violation of the provisions addressing unsolicited electronic messages).

ONLINE PRIVACY

Online privacy is governed by Canadian Privacy Statutes (discussed above). In general, Canadian privacy regulatory authorities have been active in addressing online privacy concerns.

For example, in the context of social media, the OPC has released numerous Reports of Findings addressing issues including:

- default privacy settings
- social plug-ins
- identity authentication practices, and
- the collection, use and disclosure of personal information on social networking sites. The OPC has also released decisions and guidance on privacy in the context of Mobile Apps.

In addition, the OPC has released findings and guidelines related to the use of cookies and online behavioural advertising, including findings indicating that information stored by temporary and persistent cookies is considered to be personal information and therefore subject to PIPEDA. The OPC has adopted the same position with respect to information collected in connection with online behavioural advertising.

In 'Privacy and Online Behavioural Advertising' (the 'OBA Guidelines'), the OPC stated that it may be permissible to utilize opt-out consent in the context of online behavioural advertising if the following conditions are met:

- individuals are made aware of the purposes for the online behavioural advertising, at or before the time of collection, in a manner that is clear and understandable
- individuals are informed of the various parties involved in the online behavioural advertising at or before the time of collection
- individuals are able to opt-out of the practice and the opt-out takes effect immediately and is persistent
- the information collected is non-sensitive in nature (ie not health or financial information), and
- the information is destroyed or made de-identifiable as soon as possible.

The OPC has indicated that online behavioural advertising must not be a condition of service and, as a best practice, should not be used on websites directed at children.

With respect to location data, such information, whether tied to a static location or a mobile device, is considered to be personal information by Canadian privacy regulatory authorities. As such, any collection, use or disclosure of location data requires, among other things, appropriate notice and consent. Most of the privacy regulatory authority decisions related to location data have arisen with respect to the use of GPS in the employment context.

The Canadian privacy regulatory authorities provide the following test that must be met for the collection of GPS data (and other types of monitoring and surveillance activities):

- Is the data demonstrably necessary to meet a specific need?
- Will the data likely be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained? and
- Are there less privacy-intrusive alternatives to achieve the same objective?

KEY CONTACTS

Kelly Friedman
Partner
T +1 416.369.5263
kelly.friedman@dlapiper.com

Tamara Hunter
Associate Counsel
T +1 604.643.2952
tamara.hunter@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

CAPE VERDE

Last modified 25 January 2016

LAW IN CAPE VERDE

Data Protection Law (Law 133/V/2001 (as amended by Law 41/VIII/2013) and Law 132/V/2001, of 22 January 2001.

DEFINITIONS

Definition of personal data

Personal data is defined as any information, regardless of its nature or the media on which it is stored, relating to an identifiable natural person (referred to as 'the data subject'). Natural persons are deemed to be identifiable whenever they can be directly or indirectly identified through such information.

Definition of sensitive personal data

Sensitive data is defined as personal data that refers to a person's:

- philosophical or political convictions
- party or union affiliation
- religious faith
- private life
- ethnic origin
- health
- sex life
- genetic information.

NATIONAL DATA PROTECTION AUTHORITY

The national data protection authority in Cape Verde is the *Comissão Nacional de Proteção de Dados Pessoais* ('data protection authority').

REGISTRATION

Pursuant to the Data Protection Law, before starting the processing of personal data (and considering the specific categories of personal data), prior authorization or registration with the data protection authority is required.

Specific prior written registration (ie authorization) granted by the data protection authority is necessary in the following cases:

- the processing of sensitive data (except in certain specific cases eg if the processing relates to data which is manifestly made public by the data subject, provided his consent for such processing can be clearly inferred

from his/her statements) and only in cases where the data subject has given his/her consent to the use of such data

- the processing of data in relation to creditworthiness or solvency
- the interconnection of personal data
- the use of personal data for purposes other than those for which it was initially collected.

DATA PROTECTION OFFICERS

There is no obligation to appoint a data protection officer.

COLLECTION & PROCESSING

The collection and processing of personal data is subject to the rules laid down in the Data Protection Law. As a general note, personal data processing operations may only be undertaken once the following two requirements are met:

- the express and unambiguous consent of the data subject has been obtained
- the data protection authority has been notified.

Moreover, as previously stated, there are some cases (referred to above) in which the collection and processing of personal data is subject to prior authorization from the data protection authority.

TRANSFER

The Data Protection Law stipulates that the international transfer of personal data is only permitted if the recipient country is considered to have a sufficient level of protection in respect of personal data processing.

The sufficient level of protection for foreign countries is defined by the data protection authority.

As a general rule, the transfer of personal data to countries that do not provide for an adequate level of protection of personal data can only be permitted if the data subject has given his consent or in some specific situations, namely if the transfer:

- is necessary for the performance of an agreement between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request
- is necessary for the performance or execution of a contract entered into or to be entered into in the interest of the data subject between the controller and a third party
- is necessary in order to protect the vital interests of the data subject
- is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

SECURITY

The Cape Verdean Data Protection Law stipulates that data controllers must implement technical and organizational measures so as to ensure the confidentiality and security of the personal data processed. Such obligations must also be contractually enforced by the data controller against the data processor. Moreover, certain specific security measures must be adopted regarding certain types of personal data and purposes (notably, sensitive data, call recording, video surveillance etc.).

BREACH NOTIFICATION

There is no formal requirement for breach notification, nor is there formal requirement for mandatory breach notification.

ENFORCEMENT

Enforcement of the Data Protection Law is done by the data protection authority.

Moreover, the Data Protection Law sets out criminal and civil liability as well as additional sanctions for breaches of the provisions of said statute.

Civil Liability

Any person who has suffered pecuniary or non-pecuniary loss as a result of any inappropriate use of personal data has the right to bring a civil claim against the relevant party. Criminal Liability The DPL provides that all of the following constitute criminal offences:

- a failure to notify or to obtain the authorization of the DPA prior to commencing data processing operations that require such authorization
- provision of false information in requests for authorization or notification
- misuse of personal data (ie processing personal data for different purposes than those for which the notification / authorization was granted)
- the interconnection of personal data without the authorization of the DPA
- unlawful access to personal data
- a failure to comply with a request to stop processing personal data.

These offences are punishable with a term of imprisonment of up to 2 years or a fine of up to 240 days.

Additional Sanctions

The DPL also lays down sanctions that can be imposed in addition to criminal and civil liability, namely:

- a temporary or permanent prohibition on processing data
- the advertisement of a sentence applied to a specific case
- a public warning or reproach of a data controller.

ELECTRONIC MARKETING

Law 132/V/2001 provides an opt-in right for direct marketing communications. Moreover, both Law 132/V/2001 and the Data Protection Law grant data subjects the right to object to unsolicited communications, at his/her request and free of any costs, to any data processing in relation to marketing activities.

ONLINE PRIVACY

Law 132/V/2001 lays down the legal framework for data protection in the telecommunications sector. Special rules include the following:

- any personal data obtained through phone calls performed by public operators or telecommunication public service providers must be erased or made anonymous after the phone call has ended

- traffic data can only be processed for billing, customer information or support, fraud prevention and the selling of telecommunication services.

KEY CONTACTS

CV Lexis
www.mirandalawfirm.com/

Antonio Ferreira
Partner
T +238 261 13 44
praia@cvlexis.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

CAYMAN ISLANDS

Last modified 24 January 2015

LAW IN CAYMAN ISLANDS

The Cayman Islands has not implemented a legislative framework that specifically addresses issues of data protection. There are, however, proposals to introduce a data protection regime in the Cayman Islands, potentially during the course of 2015, but the precise details and scope of any such regime are still to be finalised.

Notwithstanding the lack of specific data protection legislation, the Cayman Islands does recognise a duty of confidentiality in certain circumstances, under both the common law, and the provisions or the Confidential Relationships Preservation Law (as revised) of the Cayman Islands (the 'CRPL'). The CRPL provides a statutory framework which regulates disclosures of confidential information by professional persons, providing among other things for criminal sanctions for certain breaches of confidentiality obligations, in parallel to the civil remedies available at common law.

DEFINITIONS

Definition of personal data

There is no statutory definition of 'personal data'.

At common law, information is generally to be regarded as 'confidential' if it has a necessary quality of confidentiality and has been communicated or has become known in such circumstances as give rise to a reasonable expectation of confidence; for example if obtained in connection with certain professional relationships, if obtained by improper means, or if received from another party who is subject to a duty of confidentiality.

The CRPL does not provide an exhaustive statutory definition of confidential information, but specifies that it will include information concerning any right, interest or property, which a recipient is not, otherwise than in the normal course of business, authorised by the principal to divulge.

Definition of sensitive personal data

There is no statutory definition of “sensitive personal data”.

NATIONAL DATA PROTECTION AUTHORITY

There is currently no “Data Protection Authority” in the Cayman Islands. However, it is likely that the Cayman Islands Information Commissioner (which at present primarily addresses freedom of information issues) would be tasked with such a role in the event that a legislative data protection regime is introduced.

REGISTRATION

N/A (see National Data Protection Authority section).

DATA PROTECTION OFFICERS

There is currently no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

There are no statutory provisions that specifically address the collection and processing of personal information.

At common law, however, it is generally a breach of confidence to misuse or threaten to misuse confidential information. The concept of 'misuse' is a broad one, but will often include any unauthorised disclosure, examination, copying or taking of confidential information. The precise scope of the term however will depend largely on the specific circumstances, including the relevant relationship and the nature of the information.

In the context of confidential information received by a professional person in the context of a professional relationship with a principal, the CRPL provides that a person is guilty of a criminal offence where he or she '*clandestinely, or without the consent of the principal, makes use of*' any confidential information for his or her benefit or the benefit of another.

TRANSFER

Absent a breach of an obligation of confidentiality at common law or pursuant to the provisions of the CRPL, there is no specific regulation of the transfer of information from or within the Cayman Islands.

Notably, the CRPL is intended to have an extra-territorial effect in that it is stated to apply to confidential information that is *'bought into the [Cayman] Islands and to all persons coming into possession of such information at any time thereafter whether they be within the jurisdiction or thereout.'*

SECURITY

There are no statutory provisions mandating that specific measures be taken to protect against or prevent disclosure or other unlawful use of confidential information. However, a person who misuses or divulges confidential information (deliberately or otherwise) may be liable at common law or under the CRPL.

BREACH NOTIFICATION

There are no general requirements to notify any authority or any other person of a breach of confidentiality.

ENFORCEMENT

A breach of the common law duty of confidentiality may give rise to a claim for, among other things, damages and/or an injunction. These remedies are to be sought through, and enforced by, the courts of the Cayman Islands.

Any person in breach of a duty of confidentiality under the CRPL is guilty of a criminal offence, and is liable, on conviction, to a fine and/or imprisonment for up to four years (depending on the circumstances).

ELECTRONIC MARKETING

There are no specific restrictions addressing the use of confidential information in electronic marketing beyond those generally applicable to the use of confidential information.

ONLINE PRIVACY

There are no specific restrictions addressing online privacy of confidential information beyond those generally applicable to the use of confidential information.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Nick Bullmore
Partner
T +1 345 749 2000
nick.bullmore@careyolsen.com

Alistair Russell
Associate
T +1 345 749 2000
alistair.russell@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

CHILE

Last modified 24 January 2015

LAW IN CHILE

Personal Data Protection is addressed in several specific laws, as well as scattered provisions in related or complementary laws and other legal authority:

The main laws containing Data Protection provisions:

1. **Constitution of the Republic of Chile, Art. 19 N° 4**: establishes the 'respect and protection of the public and private life, and the honour of the person and its family'. Any person who by arbitrary or illegal act or omission suffers a deprivation, perturbation or threat to this right may file a Constitutional Protection Action.
2. **Law 19,628 'On the protection of private life', commonly referred as 'Personal Data Protection Law' (PDPL)**: mainly defines and refers to the treatment of personal information in public and private databases. Last modified: Feb. 17, 2012.
3. **Law 20,285, 'On the Access to Public Information'**: sets forth the Public Function Transparency Principle, the individual right to access the information of Public Administration bodies, and the procedures and exceptions thereof.
4. **Law 20,575: 'Establishes the Destination Principle on the Treatment of personal data'**: incorporates additional rules when treating economic and debt-related personal data.
5. **General Law on Banks, article 154, establishes the Banking Secrecy**: holds that, subject to certain specific exemptions, all deposits are secret, and related information can be given only to the account's owner or designated representative.
6. **Law 19,223, 'Criminal Conducts related to Informatics'**: establishes sanctions for those who breach and unlawfully access and/or use the information available in electronic databases.

Main Decrees containing Data Protection provisions:

1. **Decree N° 13 of 2009, Ministry of the General Secretary of the Presidency**: establishes the 'Rules' (or administrative provisions and procedures) of Law 20,285.

DEFINITIONS

Definition of personal data

Under the PDPL, 'personal data' is data referring to any information concerning natural persons, whether identified or identifiable.

Definition of sensitive personal data

Under the PDPL, sensitive personal data is data relating to the physical or moral characteristics of persons, or facts or

circumstances of their private life or intimacy, such as personal habits, racial origin, political ideologies and opinions, religious creed or beliefs, physical and mental health conditions, and sexual life.

NATIONAL DATA PROTECTION AUTHORITY

There is not one regulator who oversees matters relating to data protection and related issues; such matters are, in general, resolved by Chilean courts as follows:

- The *Jueces de Letras* - territorial civil jurisdiction, judges exercise jurisdiction in the first instance over violations of the PDPL.
- The Appeal Courts exercise jurisdiction in the first instance in connection with constitutional actions, including those involving alleged breaches of the constitutional Right to Privacy. It is also the appeals court (with second instance jurisdiction) over matters involving alleged violations of the PDPL.
- The Supreme Court hears appeals involving constitutional violations. Also, when a citizen's petition for removal, information, modification or blocking of his personal data from a public or private Database is denied on 'national security' grounds under the PDPL, it also has jurisdiction in the first instance over such claims.

REGISTRATION

Chilean law distinguishes between private and public databases containing personal data.

Private Databases: there is no registration obligation.

Public Databases: According to Article 22nd of the PDPL, and Decree 779 of 2000 of the Ministry of Justice, all public databases are administrated by the Civil Registry and Identification Service.

DATA PROTECTION OFFICERS

According to the PDPL, the 'responsible person' – ie, the natural person, legal entity, or public body that makes decisions related to the treatment of personal data – is responsible for ensuring that personal data are protected in accordance with applicable legal requirements. The 'responsible person' must also respond to the inquires of any person regarding his or her personal data, and its modification, deletion or blocking, etc. If no answer is provided by the responsible person within two business days, the affected person can initiate a civil procedure before the corresponding authorities.

When the treatment of private databases is delegated to a third party by contract, the contract must, among other things, include provisions governing record keeping, due diligence and data breaches or related losses.

COLLECTION & PROCESSING

The PDPL establishes the conditions under which personal data can be 'treated'. Similar to the definition of 'processing' in the EU, "treatment" is defined very broadly to include 'any operation or set of operations, whether automated or not, that recalls, displays, accesses, saves, records, organizes, elaborates, selects, extracts, confront, interconnects, dissociates, communicates, deletes, transfers, transmits or cancels personal data, or the use of personal data in any other form or manner'.

As a general rule, personal data can only be 'treated' when the written consent of the owner of the personal data is obtained, or when one or more of the following specific conditions are met:

1. Authorization by Law.
2. Collection from publicly accessible sources.
3. The data is of an economic, financial, banking or commercial nature, provided the further treatment of this information (including transmission or communication), meets a number of specific requirements set forth in the PDPL.

4. When data is obtained on lists related to a specific category of people, which only disclose information such as the allegiance of such individual to such specific group, his/her profession or activity, educational diplomas, address and date of birth.
5. When personal data is treated by private entities solely for their, or their associate and affiliated entities' exclusive internal use.

TRANSFER

'Transfer' is considered a form of 'treatment' of personal data. Thus, all of the aforementioned rules apply, including the consent requirements.

SECURITY

All personnel involved in treatment of personal data have a legal obligation of confidentiality related to data that is not publicly available, even after they end their contractual relation / office.

The security of personal data contained in databases is an obligation of the 'responsible person', as defined above. This person must maintain the Database, and will keep it '*with due diligence, being held accountable for the damages'.*

This is a key article, since it does not distinguish on the nature of the damages (to the Database or individuals, *moral* or common, losses, etc). While there is no actual case law interpreting this rule, it is likely to be broadly construed by a court.

If the responsible person has implemented an automated transmission procedure, it must maintain records that track:

1. the inquirer's identity
2. the motive and purpose of the request, and
3. the specific data being transferred.

BREACH NOTIFICATION

There is no obligation to provide breach notification.

ENFORCEMENT

Every data subject has the right to demand that the responsible person for a database provide information on what data is held relating to that data subject, as well as its source and any recipients, the purpose of the record, and detailed information on any persons or entities to which the data is frequently sent. A data subject may also request any incorrect or incomplete record of personal data be modified. If there is no legal justification for the recording of the personal data, a data subject may request its removal or deletion. If a data subject previously gave authorization for his or her personal data to be used for marketing, the data subject may request removal from such a marketing list.

The aforementioned rights and provisions cannot be contractually waived or limited.

However, requests for information, modification, etc. can be lawfully denied when the responsible person claims that doing so will impede its practices, will affect the duty of confidentiality, or will affect national security or interests.

In all of the above cases, if the responsible person does not reply or respond within 2 business days to a data subject's request, then the data subject can file a complaint before the local *Juez de Letras* or common civil local judge. Along with the specific claim for information, removal, etc., the affected individual can claim patrimonial and *moral* damages. The Judge must reasonably determine the amount of the reparations, and may impose a fine between US $80 – $800 (as of November, 2013). If commercial information is involved, the fine may rise up to US $4,000 (as of November, 2013.).

If the reason for denial was due to national security or interest, then the Supreme Court will assume jurisdiction over the matter.

Finally, there are also criminal sanctions (imprisonment and fines) for breaching information treatment systems and/or revealing any information contained therein.

ELECTRONIC MARKETING

The applicable provisions related to electronic marketing are set out in two laws:

Consumer Protection Law, 19.496.

Art. 4 defines 'publicity' or 'marketing' as 'the communication that the provider of goods or services sends to the public by any means, in order to inform and motivate him to purchase or contract for good or services.'All marketing practices must follow the provisions contained in the Consumer Protection Law (CPL), which are mainly two points, plus a specific provision regarding 'SPAM':

- Accuracy obligation regarding the terms and conditions and/or characteristics of the offered goods and services.
- Include an 'expedited means to request' the suspension of any further communications.
- For email marketing, every marketing email must indicate that it is an advertisement, and include the identity of the sender and a valid email address to which an opt out request may be sent.

The PDPL.

Companies are allowed to create, compile, edit, transmit, etc. databases (including telephone numbers or other contact information) for 'commercial communications', provided the personal data used for marketing is 'available from publicly accessible sources,' or the data subject has provided prior written consent.

ONLINE PRIVACY

There are no laws governing online privacy or cookies, specifically.

However, there is some risk that the use of cookies could implicate computer crime laws prohibiting unauthorized access to computers and information thereon.

KEY CONTACTS

Albagli Zaliasnik
www.az.cl/

Ariela Agosin
Partner
T +56 2 22445 6000
aagosin@az.cl

Nelson Campos
Associate
T +56 2 22445 6000
ncampos@az.cl

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

CHINA

Last modified 28 July 2016

LAW IN CHINA

Currently, there is not a comprehensive data protection law in China and instead, provisions relating to personal data protection are found across various laws and regulations. Generally speaking, provisions found in laws such as the General Principles of Civil Law and the Tort Liability Law may be used to interpret data protection rights as a right of reputation or right of privacy. However, such interpretation is not explicit. A draft Personal Data Protection Law has been under review by the government for many years, but there is still no indication as to if and when such law will be passed.

As such, the following already effective pronouncements form the backbone of general data protection laws currently in China:

- The Decision on Strengthening Online Information Protection (Promulgated and effective on 28 Dec 2012; the 'Decision') adopted by the Standing Committee of the National People's Congress, and
- National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services (Promulgated 05 Nov 2012 and effective on 01 Feb 2013, GB/Z 28828-2012; the 'Guideline') as published by General Administration of Quality Supervision, Inspection and Quarantine of China and Standardization Administration of China (Collectively referred to as 'General Data Protection Law').

The purpose of the Decision is to protect internet information security, safeguard the lawful rights and interests of citizens, legal entities or other organizations, and ensure national security and public interests. The Decision has the same legal effect as a law. Note while the Guideline is only a technical guide and thus not legally binding, is considered important because of its scope that extends to any "processing of personal information through information systems" (not necessarily connected to the internet), and because of the fact that it covers in detail key issues such as data exports, sensitive data, data subject access and the right to rectification. Given the lack of laws and regulations which provide detailed guidance on data processing, the Guideline can be a good reference. Therefore compliance with the Guideline is recommended as good practice and we thus include the Guideline in our discussion.

In addition to the abovementioned General Data Protection Law, provisions contained in other laws and regulations may be applicable depending on the industry or type of information at issue (for example, personal information obtained by banking financial institutions, e-commerce business, or telecom or internet service/content providers is subject to special regulation). In particular, recent important enactments include:

- The Criminal Law of the People's Republic of China prohibits units or individuals to sell, illegally provide or illegally access (such as theft) citizens' personal information.
- Provisions of the Supreme People's Court on Several Questions relating to the Applicable Law of Civil Disputes Concerning the Use of Informational Network to Harm Personal Rights and Interests (Promulgated on 21 August

2014, and became effective on 10 October 2014), which would be applicable to Internet users and Internet service providers who use the information network to infringe the privacy rights of a third party.

- The Provisions on Telecommunication and Internet User Personal Information Protection (Promulgated on 19 July 2013 and effective on 1 Sep 2013), which would be applicable to the telecom and Internet service providers.
- The Guidelines for the Supervision of Information Technology Outsourcing Risks of Banking Financial Institutions, which would be applicable to banks outsourcing information technology services.
- Consumer Rights Protection Law of the People's Republic of China (promulgated 25 Oct 2013 and effective on 15 Mar 2014; the 'Consumer Rights Law'), which would be applicable to most if not all types of business that deals with consumers.

A recent significant development in the legal landscape for cybersecurity and data protection in China is the Draft Cybersecurity Law ("Draft Law"). The second reading of the Draft Law took place in the first week of July 2016. Further details as to how certain terms and the draft law as a whole would be interpreted and enforced in practice are awaited, and the draft will proceed to a third reading and it's not clear when it will be passed.

The Draft Law provides a comprehensive regime for regulating cyber activities and imposes legal obligations on network service providers in relation to handling data. If enacted, the Draft Law will bear equal legislative weight as the Decision but will be of higher level of authority as compared to the Guideline.

Please note that our discussion here only includes General Data Protection Law and the Consumer Rights Law as such laws will have the most direct, general and broad application to most types if not all types of business in China. References will be made to proposed regulations stipulated in the Draft Law. Applicability of other laws or regulations will invariably depend on the factual context of each case and further independent analysis is recommended, (for example, businesses in the banking or securities sector will be subject to industry-specific data privacy related regulations).

DEFINITIONS

Definition of personal data

Under the Guideline, personal data refers to any data or information in connection with a specific individual, which can be used, separately or in combination with other data, to identify an individual.

Personal data (which is referred to as 'personal information' in the Decision) means any electronic information which can enable you to identify a citizens individual identity and which relates to personal privacy.

The Consumer Law does not provide a definition for personal data or personal information.

Under the Draft Law, personal data (which is referred to as "personal information") means personal identity information such as the name, date of birth, ID card number, biometric data, occupation, address or telephone number, which are recorded electronically or in other means, and other information which individually or collectively may serve to identify a person.

Definition of sensitive personal data

The Guideline makes distinction between personal sensitive information and personal general information. Under the Guideline, sensitive personal data (which is referred to as 'personal sensitive information' in the Guideline) is defined as personal information the leakage or alteration of which may result in adverse impact to the data subject. What is the content of personal sensitive information would depend on the intention of the data subject and the specific

characteristic of the business at hand. Examples may include personal identification number, cell phone number, race, political view, religious belief, genes or fingerprints. Personal general information is those other than personal sensitive information.

Neither The Decision nor the Consumer Rights Law makes such distinction.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in the People's Republic of China ('PRC').

REGISTRATION

The PRC does not maintain a registration of personal data controllers, personal data processing activities, or databases containing personal information.

DATA PROTECTION OFFICERS

There is no legal requirement in the PRC for organizations to appoint a data protection officer.

The Guideline however recommends that a specific institution or personnel be appointed to be responsible for the internal management of personal data privacy ('Data Controller').

COLLECTION & PROCESSING

Under the Guideline, a Data Controller should have a specific, clear and reasonable purpose when collecting personal information.

Before a Data Controller collects and process personal data, they should notify the data subject of the following:

- the purpose of processing
- collection manner and methods, specific content collected and its retention period
- scope of use, including disclosure or the scope of provision to other organization or facilities of personal information collected
- measures protecting personal information
- the name, address and contact information of the Data Controller
- the risk of providing the request personal information
- the consequences of not providing the requested personal data
- channels for submitting complaints, and
- if personal information is to be transferred or entrusted with another organization or facility, notify the data subject including but not limited to the following: purpose of transfer or entrustment, specific content and scope of use of transfer or entrustment, and the name, address, contact method of the personal information receiver or trustee.

Consent is required from the data subject before the personal information can be processed. Consent can be explicit or implicit. Implicit consent is sufficient for collection of personal general information. Explicit consent is required for collection of personal sensitive information. Where the data subject clearly objects, collection should be discontinued or the personal information should be destroyed. Furthermore, personal information should be collected on a minimally required basis in a direct manner that has been notified to the data subject. Indirect or hidden collection methods are prohibited. Also, collection from those with limited or no capacity for civil conduct (generally persons less than 16 years

old) are prohibited unless consent is acquired from their legal guardians. In case of continued collection, the data subject shall be able to customize, adjust or shut down the function of personal information collection.

The Data Controller should process personal data for the stated purpose and within the scope that the Data Controller has notified to the data subject. The Data Controller should take measures to keep the collected personal data confidential during processing and storage of the data. If the Data Controller uses a third party to process the personal data, they should inform the data subject of this fact prior to collecting the data. Furthermore, personal information should be kept in whole, usable and updated during processing. Unless in otherwise specified circumstances as stipulated in the Guideline, data subject shall have right to request for information review and modification.

Under the Decision, network service providers and other enterprises may collect and use citizen personal information when the following conditions are met:

- abide by the principles of legality, legitimacy and necessity, clearly indicate the objective methods and scope for collection and use of personal information, and obtain consent from users;
- obtain the personal information subject consents;
- satisfy the requirements established by the laws, regulations and mutual agreement; and
- disclose the rules regarding collection and use.

Article 29 of the Consumer Rights Law largely requires the same as the Decision requirements. However, Article 29 only applies to business operators collecting customer personal information (as opposed to network service providers and enterprises collecting citizen personal information).

TRANSFER

Under the Guideline, Data Controller may transfer personal data to third parties if the following conditions are met:

- the Data Controller does not transfer in contravention of the transfer purpose notified or outside the scope of transfer notified
- the Data Controller ensures, in contract, the receiver has the capability and is responsible to properly process the personal data in accordance with the Guideline
- personal data will be kept confidential from any individual, organization or facility during the transfer
- Data Controller ensures that the personal information is kept in whole, usable and updated, before and after transfer, and
- unless explicit consent from data subject, express authorization from laws or regulations or authorization from relevant authorities is acquired, personal information must not be transferred to a receiver outside the territory of the People's Republic of China.

With respect to transfers, there are no specified requirements in the Decision or the Consumer Rights Law.

The Draft Law includes requirements for personal data of Chinese citizens and "important business data" collected by KIIOs to be kept within the borders of the PRC. If there is business needs for the KIIOs to transfer these data outside of China, security assessments must be conducted. This reflects a growing trend towards data localisation in China. The definition of KIIOs remains to be finalised.

SECURITY

Under the Guideline, a Data Controller must take appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction of, or damage to, personal data.

The measures taken must ensure a level of security appropriate to the harm that may result from such unauthorized or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data.

Furthermore, the Data Controller should:

- plan, design and implement a systemic personal information management process
- design standard personal information management and implement the responsibility of managing personal information
- designate expert institution or personnel to be responsible for the internal management of personal information protection work, available to process data subject complaints or inquiries
- design and implement educational training on personal information protection
- set up an internal management control system for personal information protection, and
- periodically conduct assessment on the status of personal information safety, protection standard and measures implementation either on its own or through an independent evaluation agency.

Article 4 of the Decision requires internet service providers and other enterprises to take technical measures and other necessary measures to ensure information safety and prevent the leakage, damage, or loss of citizen electronic information collected in business activities. Where there is a risk or occurrence of information leakage, damaging or loss, remedial measures shall be taken. Article 29 of the Consumer Rights Law requires the same, though as mentioned above, the relevant provision is only applicable to business operators collecting customer personal information.

Under the Draft Law, network operators are required to establish information protection systems. In particular, network operators should take technical measures and other necessary measures to ensure the safety of the citizens' personal information and to prevent the collected data from being accidentally disclosed, tampered or destroyed. Remedial measures shall be taken immediately if personal data are being or are likely to be accidentally disclosed, tampered or destroyed. Network operators should also establish systems to handle any complaints or reports about personal data security, publish the means for citizens to make such complaints or reports, and promptly handle any such complaints or reports received.

BREACH NOTIFICATION

There is currently no mandatory requirement in PRC law that applies to the public sector to report data security breaches or losses to any authority.

The Guideline however recommend that the Data Controller should promptly notify a data breach to affected data subjects and in case of major breach, promptly report to the personal information protection management department.

Under the Draft Law, network operators must inform the data subject in the circumstances that the collected personal data are being disclosed and report must be made to the relevant authorities.

ENFORCEMENT

Sanctions in relation to data privacy breaches are scattered in different laws and regulations. Typically, it would be graded approach - warning and requirement to comply, then possibly fines up to approximately 500,000 RMB. The affected individuals may also claim for indemnification under the Tort Liability Law. In severe cases, it may lead to higher fines being imposed or the revocation of license. Responsible personnel could be prohibited from engaging in relevant business and their conduct could be recorded into their social credit files. Depending on the severity of the illegal conduct, the responsible person could be subject to detention or up to seven years of imprisonment, plus a concurrent fine to the organization if applicable.

China currently lacks an efficient and centralised enforcement mechanism for data protection and there is no data

protection authority or any other state agency established to monitor the protection of personal data. The data protection provisions provided by the Criminal Law have become the most widely used provisions to enforce privacy protection in China. Essentially, only to the illegal sale or purchase of personal data are subject to enforcement under the Criminal Law.

The Draft Law also suggest possibility of ordering corrections or issuing warnings upon discovery of violation in handling personal data. If serious or poses threat to network security, varying levels of fines between $10,000 and $500,000 may be charged, and possible suspension of permits or licenses depending on the level of non-compliance.

Please note again that the possible enforcements in light of a data privacy breach discussed here are not comprehensive in all situations, as additional laws or regulations may be applicable depending on the industry or type of information at hand.

ELECTRONIC MARKETING

Under the Decision, any organizations and individuals are forbidden from acquiring personal electronic information by theft or other illegal methods. Also, they are proscribed from selling or unlawfully providing personal electronic information to anyone else.

Network service providers will require users to provide genuine identification information when signing agreements to grant them access to the Internet, fixed-line telephone or mobile phone services or to permit users to make information public.

The Decision prohibits any organizations and personnel from sending commercial electronic information to a personal fixed-line telephone, mobile phone or email address without the consent or request of the electronic information recipient, or where the recipient has explicitly declined to receive such information. The Consumer Rights Law prohibits sending of commercial information where the customer has not consented, made any request to receive the information, or where the customer has explicitly stated refusal to receive the information.

The Cyberspace Administration of China ("CAC") has recently released the "Provisions on Administration of Internet Information Search Services". The stricter internet advertising regulation comes into force on August 1, 2016 and requires Internet search providers to ensure objective, fair and authoritative search results and remove any illegal content. Service providers are obliged to establish an information security management system to protect personal information and regularly examine the qualifications of public information. All pay-for-performance searches need to be clearly labeled on an item by item basis.

Additionally, proposals for accompanying draft rules to a draft Civil Code suggest the possibility of treating data as intellectual property. This indicates, once the law is passed, that data may be traded by organizations for marketing purposes. The draft rules may not be approved until early 2017, and the forthcoming Civil Code is expected to be approved in 2020. Further developments are awaited on these.

ONLINE PRIVACY

Article 3 of the Decision indicates that network service providers and other companies should ensure the privacy of personal electronic information. They are not allowed to disclose, falsify, damage, as well as sell or unlawfully provide personal electronic information to anyone else. Article 29 of the Consumer Rights Law offers similar protection to consumer personal information as well.

Article 5 of the Decision indicates that network service providers should strengthen management of information issued by users. Also, network service providers should stop the transmission of unlawful information and take necessary measures to remove them and save relevant records, then report to supervisory authorities.

Once citizens find network information that discloses their identity or breaches their legal rights, or are harassed by commercial electronic information, they have the right to require that the network service provider delete related information or take measures to prevent such behaviors.

In relation to online privacy on mobile apps, it is, however, required by the "Provisions on Administration of Information Services of Mobile Internet Application Programs" that app providers adopt real-name registrations and verity users' identities based on mobile phone numbers or other information. Providers are prohibited from collecting users' location data, reading their contacts, starting the recording function or camera or any other irrelevant functions without clear notification and users' consent. Furthermore, App publishers are required to undertake information content review and management mechanism including to punish anyone releasing illicit information through warnings, limitation of functions, cease updates, or shutting down accounts.

There are currently no specific requirements regarding cookies within existing laws or regulations in the PRC.

KEY CONTACTS

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

COLOMBIA

Last modified 27 January 2016

LAW IN COLOMBIA

Article 15 of the Colombian Constitution sets forth fundamental rights to intimacy, good name or reputation and data protection.

Law 1266/08 ('Law 1266'), reviewed by the Colombian Constitutional Court in Decision C 1011/08, regulates the collection, use and transfer of personal information regarding monetary obligations related to credit, financial and banking services.

Law 1581 of 2012 ('Law 1581'), reviewed by the Colombian Constitutional Court in Decision C-748/11, contains comprehensive personal data protection regulations. This law is intended to implement the constitutional right to know, update and rectify information gathered about them in databases or files, enshrined in Article 20 of the Constitution, as well as other rights, liberties and constitutional guarantees referred to in Article 15 of the Constitution.

Accordingly Law 1581 applies to:

- personal data stored in any public or private database or files
- any processing treatment of personal data in Colombia, and
- operations performed by individuals who are not located in Colombia but are subject to the jurisdiction of Colombian Law under international standards and treaties.

Under Law 1581, the data owner (data subject) must always give prior, express and informed consent for all activities pertaining the collection, use and transfer of personal data, except those that are specifically exempted from all or part of the Law, which includes the processing of credit data under Law 1266.

Decree 1377 of 2013 ('Decree 1377') which constitutes secondary regulation on data protection matters, regulates:

- authorization given by data owners for personal data treatment
- including processing treatment of sensitive data
- measures to be implemented regarding data collected before the publication of the Decree
- policies on processing treatment of personal data
- the exercise of data owner's rights
- cross border transfer and transmission of personal data, and

- liability regarding the processing of personal data through the organisational implementation of the accountability principle.

DEFINITIONS

Definition of personal data

Law 1266 defines 'personal data' as any information related to one or several identified or identifiable persons or which can be associated with an individual or a legal entity. Personal data may be public, semi private or private. Semi private data is data that is not deemed private, sensitive or public.

Under Law 1581, the definition of 'personal data' specifically includes information related to or that may be related to one or several identified or identifiable natural or legal persons.

Definition of sensitive personal data

Under Law 1266 'private data' is data that, due to its sensitive or confidential nature, is relevant only to the data owner. For example, data that pertains to the right to intimacy may be deemed sensitive data under Colombian law.

Under Law 1581 and article 3 of Decree 1377 'sensitive data' is data that relates to the intimacy of the data owner, or that, if disclosed without consent, could lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, trade-union membership, social organizations, human rights organizations, or those organizations that promote the interests of any political party or that ensure the rights and guarantees of opposition political parties, as well as data relating to health, sexual life and biometrics.

NATIONAL DATA PROTECTION AUTHORITY

Two different governmental authorities were designated as data protection authorities by Law 1266: The Superintendency of Industry and Commerce ('SIC') and the Superintendency of Finance ('SFC'). As a general rule, the SIC will be the data protection authority, unless the administrator of the data is a company that performs financial or credit activities under oversight of the SFC as set forth in applicable law, in which case the SFC will also serve as a data protection authority.

Regarding the scope of Law 1581 and Decree 1377, the data protection authority is the SIC, which, in accordance with article 19 of Law 1581 and article 26 of Decree 1377, will be responsible for monitoring the compliance of the principles, rights, guarantees and procedures provided under the law, and is entitled to require the data controllers to prove the implementation of the compliance measures provided by applicable regulation.

REGISTRATION

Law 1581 created the National Register of Databases as a public directory of all databases operating in the country.

This Register will be managed by the SIC, and may be consulted by any citizen. The Ministry of Commerce, Industry and Tourism enacted Decree 886 of 2014, as secondary regulation to Law 1581. This Decree sets out the minimum content that must be included in any entry of databases registered with this National directory, and the terms and conditions of such registry, as well as the timing requirements for the registration of databases.

A data controller must register in the National Registry any database that entails the processing of personal data. The following minimum information that must be included in the registry form:

- identification of data, location and contact data of the data controller
- identification of data, location and contact data of the data processor
- mechanisms for data subjects to exercise their rights
- name and purpose of the database
- means of processing (manual and/or automated), and

- the data processing policy.

Recently and by means of a regulation *(Circular Externa N. 2)* dated November 3, 2015 the Superintendency of Industry and Commerce enabled the Registry issuing instructions to personal data Controllers, in order to finally set into force the National Registry whereby the Controllers will have to proceed with the registry of all databases subject to Law 1581. The National Registry implies that personal data Controllers will have to submit, through the web platform created for such end, information related to the processing of the relevant databases. The National Registry does not require the submission of the databases as such.

Under the previous regulation, and until further instructions are issued, the only Controllers obliged to the National Registry by the recent instructions are (i) entities of private nature subject to registry before the Chamber of Commerce and (ii) partially state owned entities (also known as mixed public-private companies). The Superintendency of Industry and Commerce has suggested to Controllers the following registration period in order to comply with the National Registry;

LAST DIGITS OF *NIT* (by its Spanish acronym -Tax Identification Number-)	REGISTRATION PERIOD
From 00 to 24	Since 09/11/2015 up to 08/02/2016
From 25 to 49	Since 09/02/2016 up to 10/05/2016
From 50 to 74	Since 06/05/2016 up to 08/08/2016
From 75 to 99	Since 09/08/2016 up to 08/11/2016

Although the authority has suggested the above deadlines, it must be clarified as per the instructions issued data Controllers must register their databases within one year from the date in which the Superintendency of Industry and Commerce enable the Registry, and databases created after this date must be registered within two months from their creation. The Registry information must be updated by the data controller whenever material changes occur.

DATA PROTECTION OFFICERS

Neither Laws 1266 nor 1581 require organizations to appoint a data protection officer. However, data processors and data controllers are obliged to maintain adequate security levels for the protection of databases, as well as an administrative infrastructure to respond to data owners' requests and claims.

On the other hand, Decree 1377 does require organisations to appoint a person or area that will assume the personal data protection matters and that will process the exercise of the rights of the data owners. The suggestion to count with such position within the organisation has also been included in the Accountability Guide issued by the Superintendency of Industry and Commerce on May 2015. Although the content of this Guide is not binding and it was issued to support Controllers to fully comply with the obligations established by Law 1581 and supplemental regulations. The observation to the Guide will be taken into account by the Superintendency of Industry and Commerce whenever it has to examine a possible breach of Law 1581. Specifically the Guide under N.1.2 draws attention on the fact that Controllers should create a position or appoint a person in charge of privacy matters such as a Privacy Officer or Data Protection Officer.

COLLECTION & PROCESSING

Under Law 1266 and Decision C 1011, as a general rule the collection and cross border transfer of Private and Semi

private Data can be performed only with the prior consent of the data owner unless an exception applies. The exceptions, set forth in Article 5 of Law 1266, permit personal data to be disclosed or delivered directly, without consent in the following conditions:

- to the data owner or to a person to whom the owner has authorized such disclosure
- to data users
- to any judicial authority, pursuant to a judicial order
- to Government Agencies or entities, when the data is required for the performance of legal or constitutional functions
- to the Administrative Authorities who require such data for disciplinary, fiscal or administrative investigations, or
- to other databases that have the same purpose as the database of the disclosing data processor (but see Decision C 1011 below) or to databases as authorized by the data owner.

Under the interpretation in Decision C-1011, the Private and Semi Private Data of data owners may be disclosed in the foregoing cases, if the following conditions are observed: except for the disclosure to the data owner, judicial authorities, governmental agencies, and administrative authorities, the disclosure can be performed only if the data owner gives his or her prior consent, or when the data is delivered to governmental agencies, they will be deemed to act as data users and will have all the corresponding obligations which include those pertaining to confidentiality, restricted circulation, and security of data. Similarly to Law 1266, according to article 10 of Law 1581, any operation performed on personal data requires the prior, express and informed consent from the data owner except in the following cases:

- data required by a public or administrative agency in performance of their duties or required by a court order
- data that is deemed public data
- data related to medical emergencies
- data related to historical, statistical or scientific purposes, and
- data related to the Civil Registration of Persons.

Similarly, article 13 states that personal data can be disclosed without consent to the following:

- to the data owners, their successors or their legal representatives
- to any administrative authority, when the data is required for the performance of public duties, or pursuant to a judicial order, or
- to third persons to whom the owner has authorized such disclosure, or who are authorized by law.

In this regard, Decree 1377 establishes the aspects of the authorization that must be provided by the owners of the information for the processing of their personal data. The decree adds, under the concept and scope of the authorization, the need for the purposes for which the processing of data is authorized to be 'specific'. This means that the consent must be limited by the purposes of the processing, prohibiting a broad or general purpose, and thus demanding specific authorization to each one of the objectives pursued with the data processing.

In addition, Article 6 of the Decree regulates matters related to the authorization for the processing of sensitive personal data, adding the following obligations:

- to inform the owner that since the data is sensitive they are not required to authorize the processing, and
- to inform the data owner beforehand which of the data processed correspond to sensitive data and the purposes of the processing, obtaining his specific consent.

Article 10 establishes the measures to be taken by the individuals and corporations that have collected data before the Decree enactment. Among the measures to be taken, the Decree requires:

- to request the authorization of the data owners, whether employees, suppliers or customers, to continue with the processing of their personal data, informing them the policies of the treatment and how to exercise their rights as data owners, and
- to note that the purposes of processing should be the same, similar or compatible with those for which the data was originally collected and authorized.

Regarding the authorization, it is important to note that it must be obtained through efficient communication mechanisms', i.e. through media that is used in the ordinary course of interaction with the data owner (phone, email, messaging, etc.

Additionally, the new regulation sets a time limit to the processing of personal data, which corresponds to the time during which the data processing is necessary to accomplish the purposes originally authorized by the data owner. Once the purposes are fulfilled, or in the event that they disappear, the data controller shall proceed to eliminate the data collected. However, the Decree provides the possibility of keeping the data when it is necessary for compliance with legal or contractual obligations.

The Decree regulates the obligation of data controllers to develop policies for the processing of personal data and ensure that the data processor complies with the applicable standards. The Decree establishes the need for the policy to be embodied in physical or electronic means, in clear and simple language.

It determines the minimum content of the policy, which includes, among others, the processing of the data, the data owner's rights and the procedure, person or area responsible for the exercise of these rights, and the entry into force date of the policy. It further provides that any change to the policy shall be informed to the data owners before implementing the new policies.

The Decree also allows the data controllers and processors to send a privacy notice on the existence of such policies and how to access them, when they cannot make the policy available to the data owner.

TRANSFER

Under Law 1581, the cross border transfer of data is prohibited unless the foreign country where the data will be transferred meets at least the same data protection standards (adequate level of protection) as the ones provided under Colombian law. This prohibition also applies to personal data governed by Law 1266.

Adequate levels of data protection will be determined in accordance with the standards set by the Superintendency of Industry and Commerce. Regulation on this matter is still pending.

This prohibition against cross-border transfers does not apply in the following cases:

- if the data owner has expressly and unambiguously authorised the cross-border transfer of data (notice of specific elements, including destination and usage, must be given for consent to be effective)
- exchange of medical data
- bank transfers and stock
- transfers agreed under international treaties to which Colombia is a party
- transfers necessary for the performance of a contract between the data owner and the controller, or for the implementation of pre-contractual measures provided there is consent of the owner, and
- transfers legally required in order to safeguard the public interest.

In accordance with the Decree, for the international transmission and transfer of personal data, in addition to the provisions of Law 1581 of 2012, the following rules apply:

- it is not a requirement to inform the data owner about the international transmission of personal data if the transmission occurs between the data controller and the data processor, in order to process the data, as long as a data transmission agreement has been entered in between them.
- the data transmission agreement must be signed by the data controller and the data processor, and must indicate the scope of processing, the activities carried out under the data controller's liability and the obligations of the data processor towards the data owner and the data controller.

SECURITY

As mentioned, Law 1266 provides that data processors must implement security systems with technical safeguards to ensure the safety and accuracy of the data, and to prevent damage, loss, and unauthorized use or access of the data.

Similarly, Law 1581 and Decree 1377 require that data protection processors and controllers implement the necessary technical, physical, and administrative safeguards to ensure the safety of databases and to prevent their damage, loss, and unauthorized use or access.

BREACH NOTIFICATION

Article 17-N of Law 1581 requires notice to the Superintendency of Industry and Commerce of certain security risks or violations of security policies related to the management of personal data.

The Accountability Guide has established that in case an incident takes place and personal data was compromised, the controller of such data must implement mechanisms in order to notify such situation to the Superintendency of Industry and Commerce and the owner. The communication to the authority must as minimum contain:

1. type of incident;
2. date of the incident;
3. date on which the Controller found out of the incident;
4. cause;
5. type of personal data compromised (sensitive, private etc); and
6. number of data owners of whom data was compromised.

ENFORCEMENT

Superintendency of Industry and Commerce is allowed to initiate administrative investigations against those who breach the provisions of Laws 1266 or Law 1581 and to impose penalties of up to 2,000 Minimum Monthly Legal Wages (approx. US$430,000) for each case, and sanctions that include the temporary or permanent closure of the professional or commercial activities of the subject who breached the data protection regime.

The penalties under Law 1581 only apply to private entities. If an offense is committed by a public entity, the Superintendency of Industry and Commerce shall refer the action to the Attorney General's Office to initiate the respective investigation.

Additionally, on 5 January 2009 Colombia's Congress enacted Act 1273, which added an 'Information and Data Protection' criminal offence to Colombia's Criminal Code. In particular, Article 269F states: 'Violation of Personal Data: Anyone who, without being authorized to do so, to its own benefit or for a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies or uses personal codes, personal data contained in

files, archives, databases or similar means, will be held liable for imprisonment for a term of forty eight (48) to ninety six (96) months and a fine.'

Finally, data owners have the right to file, before any Colombian judge, a special constitutional action, referred to as the Constitutional Writ of Protection (Acción de Tutela) to have their fundamental right to privacy, data protection or habeas data protected.

This Constitutional Writ of Protection involves a preferential and summary proceeding under which the pertinent court must issue a decision within the 10 days following the date on which the action is filed. This means that in those cases in which the right to privacy, to intimacy or to habeas data is affected, an expeditious action could be implemented to protect the fundamental rights of the individual. In this regard, Decree 2591/91 expressly provides that an Acción de Tutela can be filed against a private individual or company that violates Article 15 of the Colombian Constitution. In general terms, a court granting an Acción de Tutela that involves habeas data will issue a decision ordering that data be rectified, updated or deleted. Failing to observe a Court's ruling could result in an imprisonment order against the defendant for a period up to 10 days.

With the enactment of Decree 1377, data controllers of personal data should be able to demonstrate at the request of the Superintendent of Industry and Commerce, the measures which have been implemented to comply with the legal obligations.

Once the request is made by the Superintendent, those responsible should provide a description of the procedures used and treatment purposes, as well as evidence of the implementation of appropriate security measures. The policies must ensure:

- the existence of an internal dependency proportional to the structure and size of the business responsible for the implementation of data protection policies
- the adoption of internal mechanisms to implement data protection policies, including training and education programs, and
- the adoption of processes for addressing and responding to inquiries, requests and complaints from data owners.

The non-compliance of the above mentioned measures is subject to the penalties described in Law 1581 of 2012.

ELECTRONIC MARKETING

Electronic Marketing is regulated by Law 527/99. The general rule is that opt-in consent from a data subject is required in order to send electronic marketing materials.

ONLINE PRIVACY

In general, consent is required to use cookies and other tracking mechanisms to collect any data that could be used to identify an individual; consent may generally be obtained via the user's acceptance to the privacy policy if the use of cookies (and the way to disable them) is fully disclosed in the privacy policy. IP address may be considered personal data; however, currently there is no official opinion or law addressing whether IP address is personal information.

Also, under the principle of access and restricted delivery enshrined in Article 4 of Law 1581, personal data may not be available on the Internet or in other mass media, unless the access is technically controllable to ensure access is available only to data owners or authorized third parties. This prohibition applies unless the information is public data, in which case its disclosure and circulation is possible within the limits established by law.

KEY CONTACTS

Gómez-Pinzón Zuleta Abogados S.A.
www.gpzlegal.com/

Mauricio Jaramillo Campuzano
Partner
T +57 1 319 2900, ext. 903
mjaramillo@gpzlegal.com

Luisa Fernanda Gutiérrez Quintero
Associate
T +57 1 319 2900, ext. 903
lgutierrez@gpzlegal.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

COSTA RICA

Last modified 27 January 2016

LAW IN COSTA RICA

The development of data privacy regulation in Costa Rica is divided among two laws (the "Laws"). The first law is Law No. 7975, *Undisclosed Information Law*, which makes it a crime to disclose confidential/personal information without authorization. The second law is Law No. 8968, *Protection in the Handling of the Personal Data of Individuals*, and its by-laws were enacted regulate the activities of companies that administer databases containing personal information. Therefore, its scope is limited.

DEFINITIONS

Definition of personal data

Personal information contained in public or private registries (e.g. medical records) that identifies or could be used to identify a natural person. Personal information can only be disclosed to persons/entities with a 'need to know' such information.

Definition of sensitive personal data

Personal information relating to ideological orientation, creed, sexual preferences. Sensitive personal data cannot be disclosed without express prior authorization from the data subject.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Law No. 8968, the Agency for the Protection of Individual's Data, hereinafter "PRODHAB", is the entity charged with enforcing compliance with the applicable regulation.

Pursuant to the abovementioned By-Laws, PRODHAB has to be granted by each data holder, for control purposes, with unrestricted and permanent access to each data base through a "Superuser". This policy has been a very controversial requirement in Costa Rica.

The Constitutional Court also has jurisdiction to hear claims alleging violations of the Laws.

REGISTRATION

Under Law 8968, companies that manage databases containing personal information and that distribute, disclose or commercialize in any manner such personal information must register before the Agency.

In-house databases are outside the scope of enforcement of the Laws.

DATA PROTECTION OFFICERS

There is no requirement for a data protection officer.

COLLECTION & PROCESSING

Any company may store and manage a database containing personal information if the following rules are respected:

- When accumulating personal information, private companies and/or the government must respect the 'sphere of privacy' to which all individuals are entitled.
- Such companies must obtain prior, express and valid consent from the owner of the personal information or its representative. Such consent must be written (either handwritten or electronic).
- Companies that maintain personal information about others in their databases must ensure that such information is:
    - materially truthful;
    - complete;
    - accurate; and
    - individuals have access to their personal data and must be entitled to dispute any erroneous or misleading information about them.

- Individuals must have access to their personal data and must be entitled to dispute any erroneous or misleading information about them at any time.
- Companies that manage databases containing personal information and that commercialize such personal information in any manner, must comply with Law 8968. Particularly, they must comply with the following:
    - Report and register the company and the database before PRODHAB.
    - Report the technical issues related to the security of the database.
    - Protect and respect confidentiality issues
    - Secure the information contained in the databases; and
    - Establishing a proceeding to review requests filed by individuals for the amendment of any error or mistakes in the database.

TRANSFER

Transfer of personal information is authorized by the Laws if the data subject provides prior, express and valid written consent to the company that manages the database. Such transfer cannot violate the principles and rights granted in the Laws.

Transferring of public information (which has general access) does not need authorization from the data subject.

SECURITY

Any company or individual using and/or managing this type of information must take all necessary steps (technical and organisational) to guarantee that the information is kept in a safe environment. If security is breached because of improper management or protection, then the responsible company may be held liable, and may be subject to penalties and civil liability for any harm.

BREACH NOTIFICATION

There is no mandatory requirement. Nonetheless, if there is a breach the entity that manages the database might be liable.

ENFORCEMENT

PRODHAB recently announced that they will begin to enforce the obligations established under the Laws. Therefore, individuals may file their claims directly to PRODHAB so they may initiate an administrative procedure against database manager.

ELECTRONIC MARKETING

General rules of data protection will apply. There is little to no regulation of electronic marketing.

Notwithstanding the above, the Telecommunications Act set the scope and the mechanisms of regulation for telecommunications (including e-marketing), by describing the data subject's rights, interests and privacy protection policy. Therefore, pursuant to such Act, marketing companies may not advertise via phone nor email unless they obtain prior and express written consent from the data subject. If such companies do not comply with such condition, they might be sanctioned with a fine that can be between 0,025% and 0,5% of the income of the company of the last fiscal year.

ONLINE PRIVACY

There has been little to no regulation in this area. However, the general rules of data protection issued by the Constitutional Court, with respect to the collection and processing of personal information, do apply.

KEY CONTACTS

FACIO & CAÐAS
www.fayca.com/

Carlos J. Oreamuno
Partner
T +(506) 2233 9202
coreamuno@fayca.com

Sergio A. Solera
Partner
ssolera@fayca.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

CROATIA

Last modified 19 October 2015

LAW IN CROATIA

Croatia implemented the EU Data Protection Directive 95/46/EC by the Personal Data Protection Law ('Official Gazette of the Republic of Croatia', nos. 103/2003, 118/2006, 41/2008 and 130/2011) ('DP Law'). The DP Law is in force as of 4 July 2003.

DEFINITIONS

Defenition of personal data

Personal data means any information relating to an identified or identifiable private individual (natural persons).

Term identifiable refers to a person that can be identified, directly or indirectly, in particular by reference to his/her personal identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Defenition of sensitive personal data

Sensitive personal data is data relating to:

- racial or ethnic origin
- political opinions
- trade union membership
- religious or philosophical beliefs
- health or sex life of a natural person, and
- personal information regarding criminal procedure and petty offence procedure.

NATIONAL DATA PROTECTION AUTHORITY

The national data protection authority is the Croatian Personal Data Protection Agency (AZOP'). AZOP has a registered seat in

Fra Grge Martica 14
Zagreb
www.azop.hr

REGISTRATION

A data controller has to inform the AZOP on its database containing personal data ('Database'). The respective information includes the Database's name, information about the controller, the data processing's purpose and legal

ground, data subjects, types of the processed data, methods of the data collection and storing, expected time period for storing and usage of the stored data, certain information on the data transfer (if any) and indication of the undertaken protection measures.

DATA PROTECTION OFFICERS

If an entity employs more than 20 employees, it has to appoint a data protection officer and to publish his/her contacts on the company's website. This appointment is to be notified to the AZOP within one (1) month. A data protection officer cannot be a person charged with violation of the company's ethical code or is under disciplinary proceedings for breach of his/her duties.

COLLECTION & PROCESSING

Collection and further processing of personal data has to be legally grounded and made only to the extent necessary for fulfilment of a specific purpose. The data subjects have to be informed on the data collected and on the purpose of its collection and processing.

Personal data has to be accurate, exact and complete. It has to be stored in a way to allow the data subject's identification, but only for the time needed to fulfil the data processing's purpose.

A data subject's consent is necessary for the legitimate processing of his/her personal data unless in certain cases prescribed by law or in particular cases explicitly prescribed by the DP Law (for example, if the processing's purpose is to fulfil the data controller's statutory obligations or to execute and realize a contract where a data subject is a contractual party, or if a data subject has published the respective data himself/herself, etc).

TRANSFER

Transfer of personal data from Croatia is allowed to the countries and international organizations with the adequate level of data protection. This adequacy is subject to the AZOP's assessment provided that the opinion of the European Commission regarding the same is, when applicable, the opinion on which the AZOP fully relies. More precisely, if the European Commission has established for a particular third country that it does not provide an adequate level of data protection, the AZOP will forbid a transfer to such country.*

On the other hand, it is considered that the countries which are signatories to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data provide the adequate level of data protection. A data controller is only to notify the AZOP of such transfers.

Under the DP Law, it is also allowed to transfer personal data to the countries or international organizations which do not provide the adequate level of data protection, but only in certain cases stipulated by the DP Law (eg when the data subject consented to the transfer or when the transfer is necessary for the protection of the data subject's life or physical integrity).

Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.

SECURITY

Personal data has to be adequately protected from abuse, destruction, loss and unauthorized changes or alterations.

A data controller has to undertake all necessary technical, personnel and organizational precautions to protect data from loss or destruction, unauthorized access, alteration, publication and every other malpractice. All data controller's

employees have to sign a confidentiality statement.

BREACH NOTIFICATION

There is no data security breach notification duty explicitly prescribed by the DP Law.

ENFORCEMENT

AZOP is competent for the enforcement of the DP Law. It monitors the legislation's implementation, determines possible malpractices, compiles a list of countries with an adequate level of data protection, conducts the Central Data Register and passes decisions in cases initiated by data subjects.

If the AZOP determines a breach of the DP Law, it can:

- issue a warning to the data controller
- order removal of the existing irregularities within certain period of time
- temporarily ban collection, processing or usage of illegally collected data
- order deletion of illegally collected data
- ban transfer of data outside of Croatia, or
- ban data processing by an outsourced data processor.

AZOP's decisions may be disputed before an administrative court.

AZOP may also propose an initiation of criminal proceedings (imprisonment up to five (5) years) or petty offence proceedings (monetary fine in range from approximately EUR 2,600 to EUR 5,200).

ELECTRONIC MARKETING

Electronic marketing is regulated by the DP Law. A data controller has to inform a data subject in advance on intention to collect and process his/her data for marketing purposes. A data subject can decline to give his/her consent for the respective processing. However, even if a data subject consents to the particular processing for the respective purposes, the processing is allowed only for as long as the data subject does not oppose the same (opt-out provisions are commonly used in consent forms).

ONLINE PRIVACY

All rules on data protection are applicable to the electronic communication and on-line privacy as well. AZOP is in charge of control of all on-line data processing.

On-line privacy and cookies are regulated by the Electronic Communications Act ('Official Gazette of the Republic of Croatia', nos. 73/2008, 90/2011, 133/2012, 80/2013 and 71/2014) which has implemented Directive 2002/58/EZ on personal data processing and privacy protection in electronic communications sector.

Usage of electronic communication network for data storage or access to already stored data in terminal data subject equipment is allowed only with a data subject's consent after he/she was clearly and completely informed on the purpose of the data processing (opt-in option).

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Danijel Pribanić
Senior Associate
T +385 1 5601 330
danijel.pribanic@karanovic-nikolic.com

Ana Bunčić
Associate
T +385 1 5601 330
ana.buncic@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

CYPRUS

Last modified 19 October 2015

LAW IN CYPRUS

Cyprus implemented the EU Data Protection Directive 95/46/EC in November 2001 with the Processing of Personal Data (Protection of the Individual) Law of 2001 and its amendments (Law No. 37(I)/2003, 105(I)/2012)).

DEFINITIONS

Definition of personal data

'Personal data' or 'data' means any information relating to a living data subject. Consolidated data of a statistical nature, from which the data subject cannot be identified, is not deemed to be personal data.

Definition of sensitive personal data

'Sensitive data' means data concerning racial or ethnic origin, political convictions, religious or philosophical beliefs, participation in a body, association and trade union, health, sex life and erotic orientation as well as data relevant to criminal prosecutions or convictions.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Commissioner for Personal Data Protection ('Commissioner')

1, iasonos Str. 2nd Floor, 1082 Nicosia, Cyprus
P.O. BOX 23378, 1682 Nicosia

T 0035722818456
F 0035722304565
commissioner@dataprotection.gov.cy

REGISTRATION

Data controllers or data protection officers who process personal data must notify the Commissioner in writing about the establishment and operation of a filing system or the commencement of processing of personal data. The information provided in this written notice is then filed in the Register of Filing Systems and Processing kept by the Commissioner and any substantial change to this information must be notified in writing without delay by the data controller or data protection officer to the Commissioner.

The notification should include the following information:

- the full name, business name or title and address of the data controller

- the address where the filing system is established or the main equipment necessary for the processing to be installed
- a description of the purpose of the processing of the personal data
- the categories of data subjects
- the categories of data which are or are intended to be processed
- the period of time for which the data will be processed or the filing system will be established
- the recipients to whom the data will be communicated
- the proposed transmissions of data to third countries and the purpose thereof, and
- the basic characteristics of the system and the measures for the security of the filing system or of the processing.

DATA PROTECTION OFFICERS

The law provides that any organisation that processes personal data must designate to the Commissioner a controller or data protection officer who is ultimately responsible for the processing of personal data.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject consents
.
- the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party
- the processing satisfies the data controller's legal obligation
- the processing protects the data controller's vital interests
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority vested in the controller or a third party to whom the data will be communicated, or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the personal data is communicated, on condition that such interests override the rights, interests and fundamental freedoms of the data subjects.

Processing of sensitive personal data is permitted when the data subject has given his explicit consent or when one or more of a list of more stringent conditions are fulfilled.

TRANSFER

Data controllers may transfer personal data out of the European Economic Area only after the data protection officer or controller has obtained a license for such transfer from the Commissioner. The Commissioner shall issue the licence only if he considers that the said country ensures an adequate level of protection.*

The transmission of personal data to a country which does not ensure an adequate level of protection, is permitted

exceptionally after a licence of the Commissioner where one or more of the following conditions are fulfilled:

- the data subject consents
- the transmission is necessary in order to protect the vital interests of the data subject
- the transmission is necessary for the conclusion and performance of a contract to which the data subject is a party
- the transmission is necessary for the implementation of pre contractual measures which have been taken in response to the data subject's request
- the transmission is necessary in order to safeguard a superior public interest
- the transmission is necessary for the establishment, exercise or defence of legal claims before a court. or
- the transmission is made from a public register which, according to the law, provides information to the public or to any person who can show legitimate interest.

Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.

SECURITY

The processing of data is confidential. It shall be conducted solely by persons acting under the authority of the data controller or the processor and only after their instructions.

Data controllers must take the appropriate technical and organisational measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. Such measures must ensure a level of security which is appropriate to the risks involved in the processing of the data.

From time to time, the Commissioner gives directions with regard to the degree of security of the data and to the measures of protection required to be taken for every category of data, also taking into account technological developments.

If the processing is performed by the processor, the assignment for the processing must be made by written contract. The assignment must provide that the processor shall perform the processing only upon instructions from the controller and that the remaining obligations set out in the relevant sections of the Processing of Personal Data Law shall also lie on the processor.

BREACH NOTIFICATION

There is no mandatory requirement in the Processing of Personal Data Law to report data security breaches or losses to the Commissioner or to data subjects.

ENFORCEMENT

The Commissioner is responsible for the enforcement of the processing of personal data law.

The Commissioner may impose on the data controller or data protection officer or their representatives or third parties the following administrative sanctions:

- a fine of up to EUR €30,000
- a temporary revocation of licence
- a permanent revocation of licence
- a warning with a specific time limit for the termination of the contravention, or
- the destruction of the filing system or the cessation of processing and the destruction of the relevant data.

Section 26 (1) of the Processing of Personal Data Law lists the breaches of the law which constitute an offence and the penalties imposed. Such penalties range from imprisonment for a term not exceeding three years or a fine up to approximately EUR €5,130 or both, to imprisonment for a term not exceeding five years or a fine up to approximately EUR €8,550 or both, depending on whether:

- the offence was caused by negligence
- the person committing the offence intended to obtain for himself or anyone else an unlawful financial benefit or cause injury to a third party, or
- the committed offence endangered the free functioning of the Government of the Republic or national security.

The offences committed in contravention of the provisions of this section 26 (1) for which no other penalty is expressly provided, are punishable with imprisonment for a term not exceeding one year or with a fine not exceeding approximately EUR €3,417.20 or by both such imprisonment and fine.

ELECTRONIC MARKETING

The Regulation of Electronic Communications and Postal Services Law of 2004 (112(I)/2004) as amended by Law ('Electronic Communications and Postal Services Law') will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an e-mail address is likely to be personal data for the purposes of the Electronic Communication and Postal Services Law).

Section 106 of the Electronic Communications and Postal Services Law states the following:

1. the use of automatic calling machines, fax, or electronic mail, or SMS messages, for the purposes of direct marketing, may only be allowed in respect to subscribers or users who have given their prior consent
2. unsolicited communications for the purposes of direct marketing, by means other than those referred to in (1) above, are not allowed without the consent of the subscribers or users concerned
3. the rights referred to in (1) and (2) above shall apply to subscribers who are natural persons. The Commissioner of Electronic Communications and Postal Regulation, may, after consultation with the Personal Data Commissioner, issue orders to safeguard that legitimate interests of legal persons, regarding unsolicited communications, are adequately protected. In 2005, the Commissioner of Electronic Communications and Postal Regulation issued the 2005 Order regarding Safeguarding the Interests of Legal Persons in relation to Unsolicited Communications, by virtue of which the protection from unsolicited communications for the purposes of direct marketing has been extended to legal persons as well
4. notwithstanding (1) above, in cases where a natural or legal person obtains from its customers contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic details for direct marketing of its own similar products or services, provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their electronic contact details when they are collected and on the occasion of each message in case the customer

has not initially refused such use, and

5. electronic mail sent for direct marketing must not disguise or conceal the identity of the sender or the person on whose behalf and/or for the benefit of the communication is made, or without a valid address to which the recipient may send a request that such communication cease.

ONLINE PRIVACY

Part 14 of the Electronic Communications and Postal Services Law deals with the collection of location and traffic data and use of cookies (and similar technologies) by publically available electronic communication service providers.

Traffic Data

Traffic Data concerning subscribers and users, which are submitted to processing so as to establish communications and which are stored by persons, shall be erased or made anonymous at the end of a call, except:

- for the purpose of subscriber billing and interconnection payments, and
- if the subscriber or user consent that the data may be processed from a person for the purpose of commercial promotion of the services of electronic communications of the latter or for the provision of added value services. Users or subscribers have the possibility to withdraw their consent for the processing of Traffic Data at any time.

The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information. Users or subscribers shall be given the possibility to withdraw their consent for the processing of Traffic Data at any time.

Location Data

Location Data may only be processed when made anonymous, or with the explicit consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

The service provider must inform the users or subscribers, prior to obtaining their consent, of the following:

- type of Location Data which will be processed
- the purpose and duration of the processing, and
- whether the data will be transmitted to a third party for the purpose of providing the value added service.

Users or subscribers shall be given the possibility to withdraw their consent for the processing of Location Data at any time.

Cookie Compliance

The storage and use of cookies and similar technologies is permitted only if the subscriber or user concerned has been provided with clear and comprehensive information, *inter alia*, about the purposes of the processing, and has given his consent in accordance with the Processing of Personal Data Law.

The above shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

KEY CONTACTS

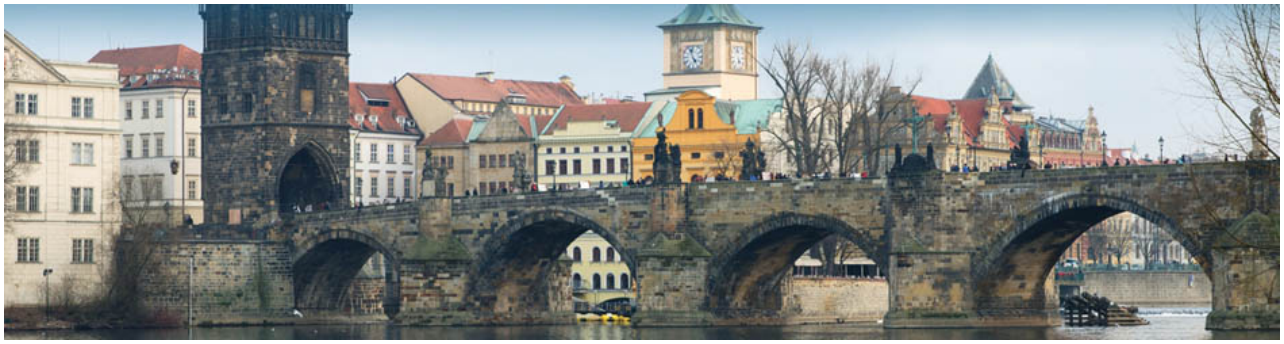
Pamboridis LLC
www.pamboridis.com/

Christy Spyrou
Partner
T +357 22 752525
spyrou@pamboridis.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

CZECH REPUBLIC



Last modified 21 January 2016

LAW IN CZECH REPUBLIC

The regulation of personal data protection in the Czech Republic is based on 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 'Data Protection Directive'). The main provisions are contained in the Act no. 101/2000 Coll., on the Protection of Personal Data, as amended (Act).

DEFINITIONS

Definition of personal data

Personal data means any information relating to an identified or identifiable data subject. A data subject shall be considered identified or identifiable if it is possible to identify the data subject directly or indirectly in particular on the basis of a number, code or one or more factors specific to his/her physical, physiological, psychological, economic, cultural or social identity.

Definition of sensitive personal data

Sensitive data means personal data revealing nationality, racial or ethnic origin, political attitudes, trade union membership, religious and philosophical beliefs, conviction of a criminal act, health status and sexual life of the data subject, as well as any genetic or biometric data of the data subject.

NATIONAL DATA PROTECTION AUTHORITY

The Office for Personal Data Protection ('Office')

Pplk. Sochora 27 170 00 Prague 7
Czech Republic

T +420 234 665 111
T +420 234 665 555
F +420 234 665 444

posta@uoou.cz
www.uoou.cz

REGISTRATION

Whoever intends to process personal data as a data controller (or change the already registered processing), shall be obliged to notify this fact in writing to the Office prior to commencing personal data processing (or change of data

processing).

The notification must include at least the following information:

- identification details of the data controller (business name, seat and identification number, and name of persons who are statutory representatives of the data controller)
- purpose of processing
- categories of data subjects and of personal data
- sources of personal data
- description of the manner of personal data processing
- location or locations of personal data processing
- recipient or category of recipients of personal data
- anticipated personal data transfers to other countries, and
- description of measures adopted for ensuring the protection of personal data.

If the notification including all required information is accepted by the Office, personal data processing may be started by a data controller after the expiration of 30 days from the delivery of the notification to the Office. In such case the Office records the information stated in the notification in the register of data controllers.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer stipulated by the Act.

COLLECTION & PROCESSING

The unequivocal (and revocable) consent of a data subject is required for the processing of personal data. Written consent is not required. However, it is recommended to obtain consent in writing, since the data controller must be able to prove the consent of a data subject during the whole period of the data processing.

Before the consent of the data subject is granted, the data subject must be clearly informed about all the aspects of processing of their personal data.

Personal data may be collected only for processing, or to be processed, if it is adequate, relevant and not excessive in relation to specific purposes for which the data is collected. Personal data may not be used for purposes which are incompatible with the reasons for which the data has been collected.

Personal data collected for different purposes may not be merged.

Personal data must be accurate and maintained up to date and it must accurately reflect the current situation of the data subject. Partially or wholly inaccurate data must be deleted or corrected.

The data controller or data processor must not disclose the personal data of the data subject to any third party without the consent of the data subject except where required or allowed to do so by law.

The personal data must be deleted once it ceases to be necessary or relevant for the purposes for which it was collected. However, where a specific law (eg the Archiving Act) sets an obligation on the data controller or data processor to keep personal data for a specific period of time, such data may not be deleted even if the data is no longer

needed for the purpose for which it has been collected and processed. However, even during such additional period of time, the personal data must be kept in a way, which will not unlawfully invade privacy and they must be anonymised.

The controller of personal data must ensure to permit the data subjects to exercise their rights of access, explication or rectification without undue delay of imprecise personal data.

Special protection rules apply in the case of processing certain 'sensitive data' relating to political views, religious and philisophical beliefs, trade union membership (this data often appears on the payroll), racial origin, health (e.g. disability, time off work due to illness, maternity leave, etc.) and sex life. Special care is required when collecting and processing such data. Explicit informed consent is generally required for the collection, processing and transfer of such data unless some of statutory carve-outs (such as the fulfilment of controller's statutory obligations, processing during the provision of health services, etc.) apply.

The personal data protection rules also apply for the processing of birth numbers. Birth numbers (a 10 digit number sequence containing information about date of birth and sex of the holder, which are given to all Czech citizens after their birth and in limited cases also to foreigners) are widely used by businesses as key identifiers (of customers, employees etc.) in databases because they provide unambiguous identification of all Czech citizens.

Although birth numbers belong among "standard" personal data (i.e. not sensitive), their use is limited by specific rules and regulations to cases specifically stipulated in Czech law or where data controllers obtain informed consent of data subjects before processing their birth numbers.

TRANSFER

There is a free flow of personal data guaranteed by the Act if personal data is transferred to a member state of the European Union.

As for personal data transfer to other countries, the Act distinguishes several different groups of data transfers.

In the first group, the Act stipulates that personal data may be transferred to other countries if the prohibition to restrict free movement of personal data ensues from an international treaty, the ratification of which was approved by the Parliament and which is binding for the Czech Republic. A typical example of such treaty is the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'.

In the second group, a personal data transfer is possible on the basis of a decision of an institution of the European Union, which basically confirms that a non-EU country sufficiently protects personal data. Among such decisions belongs, for example, the Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, or also the Commission Decision 2000/520/EC of 26 July 2000 on the adequacy of the protection provided by the safe harbour privacy principles, which allowed that data transfers to U.S. entities with so called Safe Harbour status until its abolition by the decision of the Court of Justice of the European Union no. C-362/14 on 6 October 2015.

There are also European decisions providing that personal data may be transferred without official approval under the condition that the contract includes certain standard contractual clauses set by those decisions. These decisions are for example 'Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, Commission Decision amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries' or 'Commission Decision on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC.'

Neither of the above described ways of transfer of personal data is subjected to an official approval.

In cases other than the two above described ways of transfer of personal data, controllers shall seek a prior permission of the Office to the transfer. For this purpose the controller must prove that:

- the data transfer is carried out with the consent of, or on the basis of an instruction by the data subject
- in a third party country, where personal data is to be processed, sufficient specific guarantees for personal data protection have been created
- the transfer is necessary to exercise an important public interest following from special rules and regulations or from an international treaty binding the Czech Republic
- the transfer is necessary for negotiating the conclusion or change of a contract, carried out by the data subject, or for the performance of a contract to which the data subject is a contracting party
- the transfer is necessary to perform a contract between the controller and a third party, concluded in the interest of the data subject, or to exercise other legal claims, or
- the transfer is necessary for the protection of rights or important vital interests of the data subject, in particular for saving lives or providing health care.

SECURITY

The controller and the processor are obliged to adopt adequate measures preventing unauthorised or accidental access to personal data, its alteration, destruction or loss, unauthorised transmission, other unauthorised processing, as well as other misuse of personal data. This obligation remains valid also after termination of personal data processing.

The controller or the processor are also obliged to develop and to document the technical and organisational measures adopted and implemented in order to ensure the personal data protection in accordance with the Act and other legal regulations.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the Office or to data subjects.

ENFORCEMENT

Both data controllers and data processors are jointly liable for any breach of the Act, which means that the Office and the data subjects may choose whether to hold liable just one of them or both of them.

In case of a breach of the Act, the Office may order rectification measures to be adopted and impose fines of up to CZK 5 million CZK (approx. EUR 185,000). Fines of up to CZK 10 million CZK (approx. EUR 370,000) may be imposed if:

- a substantial number of persons are jeopardised by unauthorised interference in their private and personal life, or
- obligations relating to the processing of sensitive data are breached.

A data subject who considers that there has been personal data processing in breach of the Act is entitled to complain directly to the Office.

ELECTRONIC MARKETING

When dealing with e-marketing, it is necessary to bear in mind that it is quite strictly regulated in terms of Act No. 480/2004 Col. on Certain Services of Information Society ("CSIS") as well as other previously mentioned regulations (esp. the Data Protection Directive and the Act).

CSIS states that before sending an e-mail containing marketing information, the consent of the receiver must be obtained (so called "opt-in" principle). In some cases, such as e-marketing sent to existing customers of the sender, the

consent of the customer is implied until it is withdrawn (so called "opt-out" principle). Furthermore, each such message must contain clear and visible information that any further sending of such e-mails can be rejected by the receiver together with the sender's contact information and information on whose behalf the e-mail is being sent. Last but not least, each such e-mail must be clearly tagged as a commercial message.

In order to maintain e-marketing as an effective tool, its sender should operate with good-quality databases, which enable a direct targeting of the relevant message. The sender should ensure, in particular, that (i) he will duly obtain the right to use the database for e-marketing purposes and also that (ii) personal data in the database were lawfully obtained and can be lawfully disposed of by the database owner.

When processing personal data for marketing databases, it is necessary to abide strictly by the Act. All rules described above apply to e-marketing respectively.

ONLINE PRIVACY

Online privacy is also supervised by the Office. Handling personal data is subject to the similar rules as mentioned above and specific issues are governed by Act No. 127/2005 Coll. on Electronic Communications ('AEC').

Consent to collection and processing of personal data may be expressed by electronic means, especially by filling in an electronic form.

Public electronic communication service providers are obliged to ensure the security of the personal data they process which includes technical security and creation of internal organisational regulations.

In cases of a personal data breach a public electronic communication service provider is obliged to notify the Office "without necessary delay", and in the event that the breach of protection could very significantly affect the privacy of a certain individual, such person must be notified as well.

Apart from a few exceptions, traffic data held by a public electronic communication service provider must be erased or anonymised when it is no longer necessary for the transmission of a communication.

As regards cookies, the Czech law is still using the 'opt-out' principle because the user must be informed and explicitly allowed to refuse the cookies storage (no prior consent required). The 'opt-in' principle as introduced by the Directive 2009/136/EC has not been implemented into Czech law, although many state authorities, including the Office, publicly declared the opposite. Nevertheless, due to the above-mentioned ambiguity, we cannot exclude the risk that the Office will require the prior consent to be given by visitors of the relevant web-site according to the generally applicable obligation under the Act, if the relevant cookie is able to identify the specific user.

Relevant supervising and enforcing authorities in this area are primarily the Office and to some extent also the Czech Telecommunication Office.

KEY CONTACTS

Jan Rataj
Senior Associate
T T +420 222 817 800
jan.rataj@dlapiper.com

Stanislav Bednář
Senior Associate
T T +420 222 817 310
stanislav.bednar@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

DENMARK

Last modified 12 January 2016

LAW IN DENMARK

Denmark implemented the EU Data Protection Directive 95/46/EC in June 2000 with the Act on Processing of Personal Data ('Act').

DEFINITIONS

Definition of personal data

Any information relating to an identified or identifiable natural person (data subject).

Definition of sensitive personal data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life.

NATIONAL DATA PROTECTION AUTHORITY

Datatilsynet ('DPA')
borgergade 28, 5

DK 1300 København K

T +45 3319 3200
F +45 3319 3218

REGISTRATION

Unlike most EU Member States, Denmark does not require a general registration of controllers, processing activities or databases with personal information.

However, data processors established in Denmark who offer electronic processing services must, prior to the commencement of such processing operations, notify the DPA. This notification requirement also applies to the processing of personal data which is carried out for the purpose of professional assistance in connection with staff recruitment.

Besides this notification requirement, processing of personal data must be notified by the controller to the DPA if the processing includes sensitive or other purely private data. Such a registration should include the following information:

- the name and address of the controller, his representative (if any) and the processor (if any)

- the category of processing and its purpose
- a general description of the processing
- a description of the categories of data subjects and of the categories of data relating to them
- the recipients or categories of recipients to whom the data may be disclosed
- intended transfers of data to third countries
- a general description of the security
- the date of the commencement of the processing, and
- the date of deletion of the data.

DATA PROTECTION OFFICERS

There is no requirement for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject has given his explicit consent
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of a task carried out in the public interest
- processing is necessary 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 data is disclosed, or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data is disclosed, and these interests are not overridden by the interests of the data subject.

Sensitive personal data (as detailed above) may be processed only if:

- the data subject has given his explicit consent to the processing of such data
- processing 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 consent
- the processing relates to data which has been made public by the data subject, or
- the processing is necessary for the establishment, exercise or defence of legal claims.

Personal data about purely private matters, may be processed by private entities only if:

- the data subject has given his explicit consent, or
- the processing is necessary for the purpose of pursuing a legitimate interest and this interest clearly overrides the interests of the data subject.

Personal data about purely private matters may be disclosed only if:

- the data subject has given his explicit consent, or
- the disclosure is necessary for the purpose of pursuing public or private interests, including the interests of the person concerned, which clearly override the interests of secrecy.

Furthermore, the data controller must provide the data subject with the necessary information to fulfil the duty of information, including information about the identity of the controller and the purposes of the processing for which the data is intended and any further information which is necessary having regard to the specific circumstances in which the personal data is collected and/or obtained.

TRANSFER

Data controllers may transfer personal data out of the EU/EEA if any of the following conditions are met:

- the data subject has given his explicit consent
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre contractual measures taken in response to the data subject's request
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party
- the transfer is necessary or legally required on important public interest grounds, 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
- the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case
- the transfer is necessary for the prevention, investigation and prosecution of criminal offences and the execution of sentences or the protection of persons charged, witnesses or other persons in criminal proceedings, or
- the transfer is necessary to safeguard public security, the defence of the realm, or national security.

Furthermore, data controllers may transfer personal data out of the EEA, if the data exporter and the data importer have entered into standard contractual clauses approved by the EU Commission or if the transfer is covered by Binding Corporate Rules. If the legal basis for the transfer is consent, EU standard contractual clauses, which have not been amended or Binding Corporate Rules, the transfer does not have to be notified to the DPA for approval.*

The DPA may authorise a transfer of personal data to an insecure third country where the controller adduces adequate safeguards with respect to the protection of the rights of the data subject.

**** Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for***

transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.

SECURITY

Data controllers must 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 provisions laid down in the Act. The same applies to data processors.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the DPA. However, DPA practice stresses that affected data subjects normally should be informed about breaches.

ENFORCEMENT

The DPA, which consists of a Council and a Secretary, is responsible for the supervision of all processing operations covered by the Act. If the DPA becomes aware that a data controller is in breach of the Act, the DPA can state their legal opinion.

Furthermore, the DPA can impose fines and a person who violates the Act is liable to a prison sentence of up to four months.

In addition to this, a controller shall compensate for any damage caused by the processing of personal data in violation of the Act.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act). A company can process data concerning existing customers for marketing of the company's own products if the processing is necessary for the purposes of the legitimate interests pursued by the company and these interests are not overridden by the interests of the consumer. A company may not disclose data concerning a consumer to a third company for the purpose of marketing or use such data on behalf of a third company for this purpose, unless the consumer has given his explicit consent..

According to the Danish Marketing Practices Act, a trader must not approach anyone by means of electronic mail, an automated calling system or facsimile machine with a view to the sale of products, real property, other property, labour and services unless the party concerned has requested him to do so. If a trader has received a customer's electronic contact details in connection with the sale of products or services, he may market his own similar products or services to that customer by electronic mail, provided that the customer has the option, free of charge and in an easy manner, of declining this both when giving his contact details to the trader and in the event of subsequent communications.

ONLINE PRIVACY

Directive 2009/136/EC was implemented in the new Danish Act on Electronic Communications Services and Networks which came into force on 25 May 2011 in accordance with the implementation deadline in the Directive.

According to the 'Executive Order on Information and Consent Required in Case of Storing and Accessing Information in End-user Terminal Equipment', which came into force on 14 December 2011, the use of cookies requires consent. The consent must be freely given and specific. However, this does not imply that consent must be obtained each time a cookie is used but a user must be given an option. Furthermore, the consent must be informed which implies that a user must receive information about the consequences of consenting. Finally, the consent must be an informed indication of the user's wishes. Normally, consent is obtained through tick-the-box but also the use of a homepage after having

received the relevant information concerning cookies can constitute consent. Yet, consent by use of a homepage must be used with caution.

In addition to this, the information to the user must fulfil the below mentioned requirements:

- the information must be clear and easy to understand
- the purpose of the use of the cookies must be provided
- the identity of the person or entity which is responsible for the use of the cookies must appear
- the possibility of withdrawal of consent must be easily accessible and be described in the information, and
- this information must be easily accessible for the user at all times.

KEY CONTACTS

Horten Lawfirm
www.horten.dk/

Egil Husum
Senior Associate
T +45 5234 4224
ehu@horten.dk

Heidi Steen Jensen
Junior Partner
T + 45 3334 4116
hsj@horten.dk

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

EGYPT

Last modified 22 January 2015

LAW IN EGYPT

Egypt does not have a law which regulates protection of personal data. However, there are some piecemeal provisions in connection with data protection in different laws and regulations in Egypt.

Constitutional principles concerning individuals' right to privacy under the Egyptian Constitution as well as general principles on compensation for unlawful acts under the Egyptian Civil Code govern the collection, use and processing of personal data.

In addition, the Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Some other laws provide for protection and confidentiality on certain data, such as the Egyptian Labour Law no. 12/2003 (confidentiality of the employee's file information including punishment and assessment) and the Egyptian Banking Law no. 88/2003 (confidentiality of client and account information). Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of citizens' civil status data. The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister Decree no. 465/2005 has a similar clause which provides for the confidentiality of the data of the clients of mortgage finance companies. The Egyptian Telecommunications Law no. 10/2003 provides for the privacy of telecommunications and imposes penalties which account to imprisonment in some cases on the unauthorized violation of such privacy.

Article 57 of the Egyptian Constitution promulgated in January 2014 provides for the protection of privacy and secrecy of, inter alia, mails, phone conversations and other methods of communication. The aforementioned shall not be monitored, inspected or confiscated unless by virtue of a prior court order and for a limited period of time as regulated by the law. Currently, the constitutional assembly has prepared a new version of the constitution. Article 57 of the latest draft approved by the constitutional assembly provides protection for privacy and secrecy of, inter alia, electronic mails, phone conversations and other methods of communication.

The aforementioned shall not be monitored, inspected or confiscated unless by virtue of a reasoned court order and for a limited period of time as regulated by the law. The Egyptian Constitution has not defined data protection. However, it referred to the legislative authority to regulate the communication of data in a manner that does not encroach upon the privacy of citizens, their rights and National Security.

DEFINITIONS

Definition of personal data

There is no definition of personal data or private life under Egyptian law or the New Constitution. However, Egyptian laws provide examples of the personal data that are protected such as the Labour Law. Article 77 of the Labour Law provides that the employees' files that must be kept by the employer (as mentioned below) includes the employee's personal data such as his name, job, professional skills when he joined the workplace, domicile, marital status, salary,

starting date of his work, the holiday leave he takes, punishments imposed on him and the reports of his superiors on his work.

Definition of sensitive personal data

There is no definition of sensitive personal data under Egyptian law.

NATIONAL DATA PROTECTION AUTHORITY

There is no national authority responsible for data protection in Egypt.

REGISTRATION

There is no requirement or facility to register data in a specific register.

DATA PROTECTION OFFICERS

There is no requirement in Egypt for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

According to the principles of the Egyptian Civil Code, the collection, use or processing of personal data is prohibited in case it violates the individual right to privacy and provided that such collection, use or processing constitutes a fault pursuant to the Egyptian Civil Code. A fault is defined by the judiciary as an act or omission that violates an obligation imposed by the law or assumed caution and care of the average man.

Only data which is considered pertinent to the data subject's private life requires the consent of the data subject. The competent courts will determine whether specific data is considered pertinent to the private life of the data subject or not and whether the collection or processing of such data violates an obligation imposed by the law or assumed caution and care of the average man.

Collecting data about the employee is required by law (Article 77 of the Egyptian Labour Law) which provides that each employer must keep a file for each employee which includes their personal data. Only certain persons are authorised by the law to have access to such data.

TRANSFER

The same general principles applicable to data collection and processing mentioned above apply to the transfer of data; the data controller may not transfer data pertinent to the private life of the data subject except after obtaining the consent of the data subject, unless otherwise permitted by the law.

SECURITY

Other than client and account data in banks, personal data controllers are not required by law to take specific measures against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data. The data controllers will be held liable according to the average man standard if their acts or omissions cause the processing, loss, destruction or damage to such personal data and this in turn results in damage being caused to the data subject.

BREACH NOTIFICATION

There is no mandatory legal requirement in the Egyptian law to report data security breaches or losses to the authorities or to data subjects.

ENFORCEMENT

As a general rule, civil liability may be raised in connection with violations against the individuals' right to privacy. The

prejudiced data subject should establish to the competent court the unlawful act, the damage occurred to them and the causation relationship between the unlawful act and the damage.

Civil liability for data privacy infringement has not been frequently claimed before Egyptian courts.

ELECTRONIC MARKETING

Egyptian law does not have any specific provisions which regulate Electronic Marketing.

ONLINE PRIVACY

Egyptian law does not have any specific provisions which regulate online privacy.

KEY CONTACTS

Matouk Bassiouny
matoukbassiouny.com/

John Matouk
Managing Partner
T +(202) 2795 4228/8179 (ext. 104)
john.matouk@matoukbassiouny.com

Mohamed Abdel Gawad
Senior Associate
T +(202) 2795 4228/8179 (ext. 110)
mohamed.abdelgawad@matoukbassiouny.com

Mohamed Fathy
Associate
T +(202) 2795 4228/8179 (ext. 122)
mohamed.fathy@matoukbassiouny.com

Sara Seif
Junior Associate
T +(202) 2795 4228/8179 (ext. 161)
sara.seif@matoukbassiouny.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

ESTONIA

Last modified 25 January 2016

LAW IN ESTONIA

As a member of the European Union, Estonia has implemented the EU Data Protection Directive 95/46/EC with the Personal Data Protection Act in force from 1 January 2008 ('Act').

Certain topics relating to protection of personal data and privacy are regulated under the Electronic Communications Act and the Information Society Services Act which implement Directive 2002/58 on Privacy and Electronic Communications (as amended by Directive 2009/136/EC).

Data retention requirements are established under the Electronic Communications Act, based on Directive 2006/24/EC. Even though this Directive has been declared invalid by the CJEU no relevant changes have been made in the Electronic Communications Act as a result.

The Estonian Data Protection Inspectorate has published several guidelines on its website, however such guidelines are of non binding nature.

DEFINITIONS

Definition of personal data

Personal data are any data concerning an identified or identifiable natural person, regardless of the form or format in which such data exist.

Definition of sensitive personal data

The following are sensitive personal data:

- data revealing political opinions or religious or philosophical beliefs, except data relating to being a member of a legal person in private law registered pursuant to the procedure provided by law
- data revealing ethnic or racial origin
- data on the state of health or disability
- data on genetic information
- biometric data (above all fingerprints, palm prints, eye iris images and genetic data)
- information on sex life
- information on trade union membership

- information concerning commission of an offence or falling victim to an offence before a public court hearing, or making of a decision in the matter of the offence or termination of the court proceeding in the matter.

NATIONAL DATA PROTECTION AUTHORITY

Estonian Data Protection Inspectorate (*Andmekaitse Inspektsioon*)

19 Väike Ameerika St.,
10129 Tallinn
Estonia
Telephone (+372) 627 4135
Email info@aki.ee
www.aki.ee

REGISTRATION

There is no general requirement to register data processing activities in Estonia. Registering is required only if the data processor processes sensitive personal data. Alternatively to the registration obligation, the data processor may appoint a Data Protection Officer (DPO).

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer stipulated by the Act. Data Protection Officer may be appointed as an alternative to the registration of sensitive data processing (see previous section). The Data Protection Inspectorate must be immediately informed of the appointment of such person and termination of such person's authority. Upon appointment of a person responsible for the protection of personal data, the Data Protection Inspectorate must be informed of the person's name and contact details.

COLLECTION & PROCESSING

Data controllers may generally collect and process personal data when any of the following conditions are met:

- the data subject has given his or her unambiguous consent for processing. Consent must be given in a format which can be reproduced in writing (unless adherence to such formality is not possible due to a specific manner of data processing). If the consent is given together with another declaration of intention, the consent of the person must be clearly distinguishable
- on the basis of law
- for performance of a task prescribed by an international agreement or directly applicable legislation of the Council of the European Union or the European Commission
- in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible
- for performance of a contract entered into with the data subject or for ensuring the performance of such contract (unless the data to be processed are sensitive personal data).

TRANSFER

Cross border transfers of personal data from Estonia are allowed only to countries with adequate level of data protection (ie EU/EEA member states and country whose level of personal data protection has been evaluated as adequate by the European Commission). If personal data is transferred to a country whose level of personal data protection has not been evaluated as adequate by the European Commission, a prior authorisation has to be obtained from the EDPI for such data transfer.

Cross border transfers to countries without adequate level of data protection are allowed without the authorisation of the EDPI only:

- with the consent of the data subject (please note that in the context of employment relationships, the consent is likely not considered valid)
- in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible
- if the third person requests information obtained or created in the process of performance of public duties provided by an act or legislation issued on the basis thereof and the data requested do not contain any sensitive personal data and access to it has not been restricted for any other reasons.

Unless any of the aforementioned exceptions are applicable, the data processor must obtain the prior authorisation of the Inspectorate even if the company is using the EU Standard Contract Clauses or relying on BCR-s.

SECURITY

Pursuant to the Act, the processor of personal data must implement appropriate organisational, physical and information technology security measures for the protection of personal data against accidental or intentional unauthorised alteration of the data, in the part of the integrity of data; against accidental or intentional destruction and prevention of access to the data by entitled persons, in the part of the availability of data and against unauthorised processing, in the part of confidentiality of the data.

Among others, the processor of personal data is required to keep account of the equipment and software under the control thereof used for processing of personal data, and record the following data:

- the name, type, location and name of the producer of the equipment
- the name, version and name of the producer of the software, and the contact details of the producer.

BREACH NOTIFICATION

There is no general obligation to notify data breaches.

Where the data processor is processing sensitive personal data and has appointed a person responsible of the protection of personal data (Data Protection Officer), this person has to inform the processor of personal data of a violation or breach discovered. If the processor of personal data does not take measures to terminate the violation, then the person responsible for the protection of personal data has the obligation to inform the Data Protection Inspectorate of the discovered violation.

Mandatory breach notification

Only communications undertakings are required to notify the Data Protection Inspectorate at the earliest opportunity if a data breach occurs. The notification should be done as soon as possible, but not later than 24 hours after discovering the breach. If all required information is not available, then initial information must be provided within 24 hours and additional information not later than three days after the initial notice and information was given.

ENFORCEMENT

Estonian Data Protection Inspectorate is responsible for the enforcement of personal data processing regulation. Data Protection Inspectorate may initiate supervision proceedings on the basis of a complaint or on its own initiative.

The processor of personal data may bear liability in misdemeanour proceedings where a fine of up to EUR 32,000 may be imposed.

As part of administrative supervision the Estonian Data Protection Inspectorate has the right to:

- suspend the processing of personal data
- demand the rectification of inaccurate personal data
- prohibit the processing of personal data
- demand the closure or termination of processing of personal data, including destruction or forwarding to an archive
- where necessary, immediately apply, in order to prevent the damage to the rights and freedoms of persons, organisational, physical or information technology security measures for the protection of personal data pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act, unless the personal data are processed by a state agency.

Officials of the Data Protection Inspectorate have the right to issue precepts to processors of personal data and adopt decisions for the purposes of ensuring compliance with the Act. Upon failure to comply with a precept, the Data Protection Inspectorate may impose a penalty payment in administrative proceedings. The upper limit for a penalty payment is EUR 9,600 and this penalty payment may be imposed repeatedly until the non compliance is removed.

ELECTRONIC MARKETING

Electronic marketing is regulated by the Electronic Communications Act. As a general rule, the data subject must be able to consent to the electronic marketing. The requirements for this consent depend on whether the addressee is a natural or a legal person, and whether there is an existing client relationship between the parties. Real time non automated phone calls and regular mail are not considered electronic marketing under Estonian law.

In addition, the customer consent must be obtained separately from other terms of the contract between the parties – ie it cannot be obtained in the standard terms presented to the customer (eg 'By accepting these terms you agree to receive our commercial communication to the email provided to us'). For example, in practice a checkbox separate from the acceptance of the standard terms is often used to obtain this consent.

Opt-in is required if the addressee is a natural person, except in the case of an existing client relationship, where opt out is permissible. The message itself must always include information to clearly determine the person on whose behalf the marketing is sent, clearly distinguishable direct marketing information and clear instructions on how to refuse from receiving further direct marketing (eg an unsubscribe link).

Reliance on an opt-out (for natural persons) in the framework of existing client relationships is subject to the following additional requirements:

- the same entity has obtained the contact details in the course of a sale
- the direct marketing is in respect of similar goods or services
- the recipient was given a possibility to opt out at the collection of his/her personal data
- the message must include information to clearly determine the person on whose behalf the marketing is sent
- the message must include clearly distinguishable direct marketing information and the recipient is given a simple means in each subsequent email to opt out/unsubscribe.

If the addressee is a legal person, then opt out system is applicable. There is no need to obtain a prior consent for direct marketing, but:

- the message must include information to clearly determine the person on whose behalf the marketing is sent

- the message must include clearly distinguishable direct marketing information
- the recipient is given a simple means in each subsequent email to opt out/unsubscribe.

ONLINE PRIVACY

Traffic data and location data

Traffic data retention requirements apply only to communications undertakings. Providers of telephone or mobile telephone services and telephone network and mobile telephone network services, as well as providers of Internet access, electronic mail and Internet telephony services are required to preserve for a period of one year network traffic data, location data and associated data thereof which is necessary to identify the subscriber or user in relation to the communications services provided.

Cookies

Due to opt out system consent to cookies is not needed. The law does not refer specifically to browser settings or other applications to be adopted in order to exercise the right to refuse. We note that a draft law has been initiated under which an opt in system for cookies will be applicable to providers of information society services. The amendment was initially planned to enter into force on 1 June 2015, but currently there is no clear indication regarding the possible enforcement date.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kaupo Lepasepp
Partner
T +372 6 400 900
kaupo.lepasepp@sorainen.com

Mihkel Miidla
Senior Associate, Head of Technology & Data Protection
T +372 6 400 959
mihkel.miidla@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

FINLAND

Last modified 1 April 2016

LAW IN FINLAND

Finland is a member of the European Union and has implemented the EU Data Protection Directive 95/46/EC with the Personal Data Act 523/1999 ('Act') (*Henkilötietolaki*) in June 1999.

Other important Finnish laws concerning data privacy and protection are the Code for Information Society and Communications Services 917/2014 ('Information Society Code') (*Tietoyhteiskuntakaari*) of 1st January 2015, which aims to inter alia ensure the confidentiality of electronic communication and the protection of privacy, and the Act on the Protection of Privacy in Working Life 759/2004 ('Working Life Act') (*Laki yksityisyyden suojasta työelämässä*), which aims to promote the protection of privacy and other rights safeguarding the privacy in working life.

Information Society Code is an ambitious effort to collect the relevant laws relating to information society under a single statute. The Information Society Code contains mostly the same provisions as the preceding laws, but it combines a large quantity of different provisions under a single law and covers a large area of legislation.

The Working Life Act includes some specific provisions on privacy issues relating to employment and work environments such as right to monitor employees' email communication.

DEFINITIONS

Definition of personal data

'Personal data' means "any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household".

Definition of sensitive personal data

Personal data is deemed sensitive "if it relates to or is intended to relate to:

- race or ethnic origin;

- the social, political or religious affiliation or trade-union membership of a person;
- a criminal act, punishment or other criminal sanction;
- the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person;
- the sexual preferences or sex life of a person; or
- the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person."

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Ombudsman (*Tietosuojavaltuutettu*) is the local supervisory authority.

Post address:

P.O. Box 800

00521 Helsinki

Finland

Visiting address:

Ratapihantie 9, 6th floor

T +358 29 56 66700

tietosuoja@om.fi

www.tietosuoja.fi

REGISTRATION

The Act imposes an obligation for data controllers to make a notification to the Data Protection Ombudsman only in certain limited situations. The data controllers have the obligation to make a notification in case of automated processing of personal data and any other processing of personal data provided that the processed personal data constitutes or is meant to constitute a personal data file. The other situations include e.g. outsourced processing of personal data, direct marketing or survey business activities and certain situations where personal data is transferred outside the European Union or the European Economic Area. The exemptions where notification to the Data Protection Ombudsman is not necessary are further specified in the Act. As the obligation to notify is currently set relatively narrow, the exemptions of the Act cover the majority of the practical situations of data processing.

The Act, however, includes an obligation to the data controllers to draw up description of their personal data file. According to Section 10 of the Act, the data controller "shall draw up a description of the personal data file, indicating:

- the name and address of the controller and, where necessary, those of the representative of the controller;
- the purpose of the processing of the personal data;
- a description of the group or groups of data subjects and the data or data groups relating to them;
- the regular destinations of disclosed data and whether data are transferred to countries outside the European Union or the European Economic Area; and
- a description of the principles in accordance to which the data file has been secured."

With some minor exceptions, the description must be kept so that anyone may access it.

DATA PROTECTION OFFICERS

The Act does not currently include a specific obligation for organisations, businesses or other entities to have a special data protection officer appointed, but organisations, businesses and other entities processing personal data should name a specific contact person in the description of the personal data file.

COLLECTION & PROCESSING

Data controllers may only collect and process personal data if:

- the data subject has unambiguously consented to the processing;
- the data subject has given an assignment for the processing, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
- processing is necessary, in an individual case, in order to protect the vital interests of the data subject;
- processing is based on the provisions of an Act or it is necessary for compliance with a task or obligation to which the controller is bound by virtue of an Act or an order issued on the basis of an Act;
- there is a relevant connection between the data subject and the operations of the controller, based on the data subject being a client or member of, or in the service of, the controller or on a comparable relationship between the two (connection requirement);
- the data relate to the clients or employees of a group of companies or another comparable economic grouping, and they are processed within the said grouping;
- processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the controller;
- the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business, and the data is processed in order to safeguard the rights and interests of the controller or a third party receiving the data; or
- the Data Protection Board has issued permission for the processing, as provided in the Act.

In addition to the requirements described above, separate requirements cover the processing of personal identity numbers and sensitive personal data. Processing of sensitive personal data is forbidden except in specific situations described in the Act.

Purposes for the processing of the personal data as well as where the personal data will be acquired from, and where it will be transferred to, must be defined in advance by the data controller. Personal data must not be used or processed in a manner incompatible with the purposes defined by the data controller. In general, personal data must only be used and processed to the extent necessary and the data controller must follow a duty of care when processing personal data.

When the data controller collects personal data, the data controller must ensure that the data subject can have information on the controller and, where necessary, the representative of the controller and on how to proceed in order to make use of the rights of the data subject in respect to the processing of the personal data.

TRANSFER

Personal data may be transferred outside the European Union and the European Economic Area only if the level of data protection in such country is sufficiently guaranteed. The sufficiently guaranteed level of protection in third countries is defined according to the decisions made by the European Commission pursuant to the Data Protection Directive.

In other situations personal data may be transferred outside the European Union and the European Economic Area if any of the below mentioned conditions are met:

- the data subject has unambiguously consented to the transfer;
- the data subject has given an assignment for the transfer, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
- the transfer is necessary in order to make or perform an agreement between the controller and a third party and in the interest of the data subject;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is necessary or called for by law for securing an important public interest or
- for purposes of drafting or filing a lawsuit or for responding to or deciding such a lawsuit;
- the transfer is made from a file, the disclosure of data from which, either generally of for special reasons, has been specifically provided in an Act;
- the controller, by means of contractual terms or otherwise, gives adequate guarantees of the protection of the privacy and the rights of individuals, and the Commission has not found, pursuant to Articles 3 and 26(3) of the Data Protection Directive, that the guarantees are inadequate; or
- the transfer is made by using standard contractual clauses as adopted by the Commission in accordance with Article 26(4) of the Data Protection Directive.

Prior to the Court of Justice of the European Union's judgment in the Schrems case (C-362/14), transfer of personal data from Finland to the United States was allowed in compliance with the US/EU Safe Harbour principles. Currently data transfers from Finland to the United States are only allowed following the instructions and directions given by the

European Commission as the safe harbour regime is no longer regarded as valid. The current instructions concern transfers on basis of alternative data transfer methods, such as contractual solutions using the European Commission's model standard clauses and binding corporate rules for intra-group transfers.

The European Commission is currently negotiating with the United States authorities to find new solutions for data transfers. However, the Article 29 Working Party stressed that an appropriate solution needs to be found by the end of January 2016 or the Data Protection Authorities will have to take necessary actions. The Article 29 Working Party is currently also assessing the acceptability of the above mentioned alternative data transfer methods.

SECURITY

The data controller is obligated to implement the necessary technical and organisational measures to protect and secure personal data against any unauthorised access as well as against any unlawful or accidental disclosure, manipulation, destruction, or other unlawful processing. The available techniques, associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy should be considered when the data controller carries out the measures.

Anyone operating on behalf of the data controller shall, before starting to process data, provide the controller with appropriate clearances and commitments as well as any other adequate guarantees of the security of the data as provided in the Act.

BREACH NOTIFICATION

The Act does not include any mandatory requirement to report breaches of data security or losses of data to the data subject or the data protection authorities. Even though the Act does not currently include any such mandatory obligation, the Data Protection Ombudsman may give instructions to the data controller to take necessary measures (in data breach or loss situations), which may include an obligation to notify the data subjects of the breach.

ENFORCEMENT

The Data Protection Ombudsman directs and supervises the enforcement of the Act together with the Data Protection Board. The Data Protection Ombudsman provides guidelines and advice on processing and transfer of data according to the applicable legislation, and may also refer data protection related matters to the Data Protection Board or report it to prosecution.

The Data Protection Board has the power of decision in data processing matters referred to it by the Data Protection Ombudsman. The Data Protection Board may:

- prohibit processing of personal data which is contrary to the provisions of this Act or the rules and regulations issued on the basis of this Act;
- compel the person concerned to remedy an instance of unlawful conduct or neglect;
- order that the operations pertaining to the file be ceased, if the unlawful conduct or neglect seriously compromise the protection of the privacy of the data subject or his/her interests or rights, provided that the file is not set up under a statutory scheme; and
- revoke permission for the processing of personal data granted by the Data Protection Board, where the prerequisites for the permission are no longer fulfilled or the controller acts against the permission or the rules attached to it.

The Data Protection Board as well as the Data Protection Ombudsman may impose a penalty payment to ensure the compliance with the Act and/or the decisions of the Data Protection Ombudsman and the Data Protection Board. Criminal liability may also ensue from the failure to comply with the Act under the Finnish Penal Code 38/1889 (*Rikoslaki*) or the Act. According the Finnish Penal Code, the failure to comply with the Act may be punished with fines or even up to one year of imprisonment.

ELECTRONIC MARKETING

The Information Society Code regulates direct marketing by electronic means in Finland. The Data Protection Ombudsman is the supervising authority also in compliance issues with the Information Society Code's provisions concerning direct marketing.

Direct marketing to natural persons is only allowed by means of automated calling systems, facsimile machines, or email, text, voice, sound or image messages and only if the natural person has given his/her prior consent to it. Direct marketing using other means is allowed if the natural person has not specifically forbidden it. If, however, a service provider receives an email address, number or other contact information in relation to the sale of product or service, the service provider may normally use this contact information to directly market the service providers own products or services belonging to the same product group or that are otherwise similar to the natural person in question. The natural person must be able to easily and at no charge forbid any direct marketing and the service provider must clearly inform the natural person of that possibility.

A service provider may use direct marketing with legal persons unless they have specifically forbidden it. As with natural persons, legal persons must also be able to easily and at no charge forbid any direct marketing and the service provider must clearly inform the legal person of that possibility. In addition, telecommunications operators and corporate or association subscribers are entitled, at a user's request, to prevent the reception of direct marketing.

The Data Protection Ombudsman and the Finnish Customer Marketing Association have given their interpretations on B2B direct marketing using a legal person's general contact information, such as an email address (e.g. info@company.com). If the B2B direct marketing is sent to a legal person's employee's personal work email (fistname.lastname@company.com), the person's prior consent is required unless the marketed product or service is substantially related to the person's work duties based on the person's job description.

Email, text, voice, sound or image message sent for the purpose of direct marketing must be clearly and unmistakably be recognised as direct marketing. It is forbidden to send such a direct marketing message that:

- disguises or conceals the identity of the sender on whose behalf the communication is made;
- is without a valid address to which the recipient may send a request that such communications be ended;
- solicits recipients to visit websites that contravene with the provisions of the Consumer Protection Act 20.1.1978/38 (*Kuluttajansuojalaki*).

If any processing of personal data is involved in the electronic direct marketing, the provisions of the Act will also apply. This means that the data subject may prohibit the use of his/her personal data for advertising or marketing purposes,

and that the personal data may only be collected into a data file in accordance with the provisions of the Act.

ONLINE PRIVACY

The Information Society Code regulates online privacy matters such as the use of cookies and location data.

Cookies

A service provider is allowed to save cookies and other data in a user's terminal device, as well as use such data, only with the consent of the user. The consent can be given via web browser or other applicable settings. The service provider must also give the user clear and complete information on the purposes of use of cookies.

However, the above restrictions do not apply to use of cookies only for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

Location Data

The location data associated with a natural person can be processed for the purpose of offering and using added value services, if;

- the user or subscriber, whose data is in question, has given his/her consent;
- if the consent is otherwise clear from the context; or
- is otherwise provided by law.

In general, location data may only be processed to the extent necessary for the purpose of processing and it may not limit the privacy any more than absolutely necessary.

The value added service provided shall ensure that:

- the user or subscriber located has easy and constant access to specific and accurate information on his/her location data processed, purpose and duration of its use and if the location data will be disclosed to a third party for the purpose of providing the services:
- the above mentioned information is available and accessible to the user or subscriber prior him/her giving his/her consent;
- the user or subscriber has the possibility to easily and at no separate charge cancel the consent and ban the processing of his/her location data (if technically feasible).

The user or subscriber is entitled to receive the location data and other traffic data showing the location of his/her terminal device from the value added service provider or the communications provider at any time.

KEY CONTACTS

Markus Oksanen
Partner
T +358 9 4176 0431
markus.oksanen@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

FRANCE

Last modified 21 January 2016

LAW IN FRANCE

Law No. 78 17 of 6 January 1978 on 'Information Technology, Data Files and Civil Liberty' ('Law') is the principal law regulating data protection in France.

The EU Data Protection Directive 95/46/EC was implemented via Law No. 2004-801 of 6 August 2004 which amended the Law.

Enforcement of the Law is principally through the '*Commission Nationale Informatique et Libertés*' ('CNIL').

DEFINITIONS

Definition of personal data

Any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him or her such as a name, registration number, telephone number, etc.

Definition of sensitive personal data

Personal data that reveals directly or indirectly, racial and ethnic origins, political, philosophical or religious opinions or trade union affiliation of persons, or that concern their health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

Commission Nationale de l'Informatique et des Libertés (CNIL)

8, rue Vivienne
CS 30223
75083 Paris Cedex 02

T 01 53 73 22 22
F 01 53 73 22 00

http://www.cnil.fr/english/

The CNIL is responsible for ensuring that information technology remains at the service of citizens, and does not jeopardise human identity or breach human rights, privacy or individual or public liberties.

REGISTRATION

Except for certain data processing that is subject to exemption, authorisation, ministerial order or decree issued by the Supreme Administrative Court (Conseil d'Etat), the processing of personal data requires a prior declaration to the CNIL.

The prior declaration to the CNIL shall specify, amongst other things:

- the purpose(s) of the processing
- the identity and the address of the data controller (ie the natural or legal person who determines the purpose and the means of the personal data processing and implements such decisions itself or appoints a data processor to implement them)
- the interconnections between databases
- the types of personal data processed and the categories of persons concerned by the processing
- the recipients of the processed data
- the time period for which the data will be kept
- the department or person(s) in charge of implementing the data processing
- the recipients or categories of recipients of the personal data
- the measures taken in order to ensure the security of the processing, and
- the existence of a data transfer to a country outside of the EU regarded by the CNIL as not providing an adequate level of protection.

The CNIL may also exempt certain processing from prior declaration, in view of their purposes, addressees, the nature of the processed data, the length of its retention or the concerned persons. Other processing may require only a simplified prior declaration.

DATA PROTECTION OFFICERS

There is no legal requirement for organisations to appoint a data protection officer ("DPO", known as a "Correspondant Informatique et Libertés" or "CIL" in France).

However, an organisation is exempt from making prior declarations to the CNIL if the organisation has appointed a DPO.

The appointment of a DPO does not exempt an organisation from requesting prior authorisation, where necessary (eg transfer of data to a country that does not provide an adequate level of protection to personal data).

The DPO is in charge of verifying the compliance of data processing with the Law. The DPO communicates, to any person who requests, information on the processing such as its purposes, interconnections, the types of data and the categories of concerned persons, the length of data retention and the department in charge of implementing the processing.

COLLECTION & PROCESSING

Any personal data must be processed in a manner consistent with the following general principles:

- all personal data is processed fairly and lawfully
- all personal data is collected for specific, explicit and legitimate purposes and are subsequently processed in

accordance with these purposes

- all personal data collected is adequate, relevant, and non-excessive in view of the purposes for which they are collected
- all personal data is accurate, comprehensive and, when necessary, kept up to date, and
- all personal data is retained for no longer than is necessary for the purposes for which it is processed.

The processing of personal data shall have received the individual's consent or shall fulfil one of the following conditions:

- compliance with a legal obligation incumbent on the data controller
- the purpose of the processing is to protect the individual's life
- the purpose of the processing is to carry out a public service
- processing relates to the performance of a contract to which the concerned individual is a party, or pre-contractual measures requested by that individual, or
- processing relates to the realisation of the legitimate interest of the data controller or of the data recipient, subject to the interest and fundamental rights and liberties of the concerned individual.

Where sensitive personal data is processed, a different list of specific conditions applies.

Whichever of the above conditions is relied upon, the person from whom the personal data is collected must be informed of:

- the identity of the data controller and, as the case may be, its representative
- the purposes of the data processing
- the recipients or categories of recipients of the data
- whether it is required to provide personal data, and the consequences of not providing data
- the right to object, for a legitimate purpose, to the collection of such data, a right to access the collected data and a right to have the processed data rectified, completed, blocked or deleted, and
- where data is to be transferred outside the EU, specific details on what, where and why the data is transferred and under which level of protection.

TRANSFER

Transfer of a data subject's personal data to a non EU/European Economic Area country is allowed if the country guarantees to individuals a sufficient level of protection in terms of privacy and fundamental rights and liberties. The sufficient nature of the protection is assessed taking into account national laws, applicable security measures, specific characteristics of the processing, such as its purpose and duration, as well as the nature, origin and destination of the processed data.

Data controllers may transfer personal data out of the European Economic Area to countries that are not deemed to offer adequate protection if the transfer is necessary:

- for the protection of the individual's life
- for the protection of the public interest

- to comply with obligations allowing the acknowledgement, the exercise or the defence of a legal right
- for consultation of a public register intended for the public's information
- for the performance of a contract between the data controller and the individual, or pre contractual measures undertaken at the individual's request, or
- for the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party

The CNIL may allow transfers if the above conditions are not fulfilled provided there is an adequate level of protection by reason of contractual provisions eg by standard contractual clauses (Model Clauses) approved by the European Commission, or internal rules (Binding Corporate Rules) applicable to data exporter and data importer.

Following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14), the CNIL no longer considers the US-EU Safe Harbor regime as a valid basis for transferring personal data to the US. Consequently, the CNIL has launched an information campaign and notably contacted controllers informing them that they have until 31 January 2016 to amend their existing CNIL declarations to either declare that their data transfers to the U.S. have ceased, or to indicate that the data transfers will be based on another data transfer mechanism (Model Clauses or Binding Corporate Rules - which the CNIL considers can still be used, subject to the assessment of these transfer tools by the Article 29 Working Party - or other exceptions to the prohibition on transfer of personal data outside the EU). If no alternative basis for transfer is declared to the CNIL by the end of January 2016, the CNIL will assume that transfers of personal data to the U.S. have stopped.

SECURITY

The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, amongst other things, prevent alteration, corruption or access by unauthorised third parties.

A data processor may only process personal data on behalf and upon instruction given by the data controller. The data processor must provide sufficient guarantees in terms of security and confidentiality, but even if this is the case, the data controller remains liable for compliance with these obligations.

BREACH NOTIFICATION

The Law does not set out any general obligation to notify the CNIL or the data subject in the event of a data security breach.

However, electronic communication services providers must notify the CNIL without delay in the event of a data security breach during the provision of electronic communications services via publicly available electronic communications networks. The breach must also be notified without delay to subscribers if it may violate their personal data or privacy, except if the CNIL has already established that appropriate protection measures have been implemented by the provider in relation to the data implicated by the breach.

Electronic communication services providers must keep up to date an inventory of all breaches of personal data.

ENFORCEMENT

The CNIL has the power to proceed with verifications of any data processing, and, as the case may be, to request a copy of every document that it considers useful in view of its mission. Since March 2014, CNIL agents are authorised to

perform online inspections and issue compliance orders to companies in violation with the Law. The data controller is only informed of the investigation once it has been conducted. In addition, agents of the French Competition Authority are authorized, within the scope of their investigation, to report violations of the Law to the CNIL.

The CNIL also has the power to pronounce different sanctions that vary in accordance with the severity of the violation committed by the data controller:

- warnings and notices to comply with the obligations defined in the Law, and
- if the data controller does not comply with the notice, the CNIL has the power to order a financial sanction up to EUR 150,000 for the first violation, and in the case of a second violation in the following 5 years, up to EUR 300,000 and/or to order that the company immediately cease the data processing.

In accordance with Articles 226-16 to 226-24 of the French Criminal Code, various violations of the Law may constitute a misdemeanour. For example, the violation, even by negligence, of the prior declaration requirements (see Registration above) is punishable by up to 5 years' imprisonment, and/or a fine of up to EUR 300,000 (for natural persons), or a fine up to EUR 1.5M and/or other sanctions (for legal persons).

ELECTRONIC MARKETING

The Act does not contain explicit provisions with respect to electronic marketing. However, Article L. 34-5 of the French Postal and Electronic Communications Code regulates electronic marketing in France. The CNIL has issued guidelines on the basis of this provision.

The CNIL distinguishes between B2B and B2C relationships.

In any event, all electronic marketing messages must specify the name of the advertiser and allow the recipient to object to the receipt of similar messages in the future.

Electronic marketing to consumers (B2C)

Electronic marketing activities are authorised provided that the recipient has given consent at the time of collection of his/her email address.

This principle does not apply when:

- the concerned individual is already a customer of the company and if the marketing messages sent pertain to products or services similar to those already provided by the company, and
- the marketing messages are not commercial in nature

In any event the concerned individual, at the time of collection of his/her email address:

- be informed that it will be used for electronic marketing activities, and
- be able to easily and freely object to such use.

Electronic marketing to professionals (B2B)

Electronic marketing activities are authorised provided that the recipient has been, at the time of collection of his/her email address:

- informed that it will be used for electronic marketing activities, and
- able to easily and freely object to such use.

The message sent must relate to the concerned individual's professional activity.

Please note that email addresses such as *contact@companyname.fr* are not subject to prior consent and right to object.

ONLINE PRIVACY

Cookies

The EU Cookie Directive has been implemented in the Law. It states that any subscriber or user of electronic communications services must be fully and clearly informed by the data controller or its representative of:

- the purpose of any cookie (ie any means of accessing or storing information on the subscriber's/user's device, eg when visiting a website, reading an email, installing or using software or an app), and
- the means of refusing cookies

unless the subscriber/user has already been so informed.

Cookies are lawfully deployed only if the subscriber/user has expressly consented after having received such information. Valid consent can be expressed via browser settings if the user can choose the cookies he/she accepts and for which purpose.

However, the foregoing provisions do not apply:

- to cookies the sole purpose of which is to allow or facilitate electronic communication by a user
- if the cookie is strictly necessary to provide on line communication services specifically requested by the user.

In December 2013 the CNIL issued updated recommendations for cookies that are more flexible than the CNIL's prior position. The CNIL considers that certain cookies are not covered by the Law (eg cookies used to constitute a 'basket' on a e-commerce platform, session ID cookies authentication cookies, certain analytics cookies, etc.).

Regarding consent, the CNIL has specified that consent must be:

- freely given (ie in circumstances where the user has a choice to refuse consent)
- specific (ie relate to a specific cookie associated with a clearly defined purpose)
- informed (ie the user must be given information beforehand, specifying the cookie's purpose as well as the possibility to revoke consent).

The CNIL regards the following consent collection mechanisms as compliant:

- a banner on the first webpage visited (of a particular site), which can specify eg that continuing to visit the site constitutes consent to set cookies
- a consent request zone overprinting on the site's homepage
- boxes to tick when registering for an online service
- buttons that activate functionalities of services that set cookies (such as plugins on social networks)

The CNIL considers that the obligation of obtaining the user's prior consent is incumbent on website publishers, mobile application publishers, advertisers ("*régies publicitaires*"), social networks, analytics services providers, etc., which must all comply with the Law, whether they deploy or read cookies on their own or a third party website or application.

Since October 2014, the CNIL has started to verify compliance with its recommendations on cookies and tracking technologies through onsite and online inspections, which resulted in a number of formal notices to comply with the Law.

Location and Traffic Data

The Postal and Electronic Communications Code deals with the collection and processing of location and traffic data by electronic communication service providers ('CSPs').

All traffic data held by a CSP must be erased or anonymised. However, traffic data may be retained eg:

- for the purpose of finding, observing and prosecuting criminal offences
- for the purpose of billing and payment of electronic communications services
- for the CSP's marketing of its own communication services, provided the user has given consent thereto.

Subject to exceptions (observing and prosecuting criminal offences; billing and payment of electronic communications services), location data may be used in very limited circumstances, eg:

- during the communication, for the proper routing of such communication
- where the subscriber has given informed consent, in which case the location data may be processed and stored after the communication has ended. Consent can be revoked free of charge at any time.

KEY CONTACTS

Carol A.F. Umhoefer
Partner
T +331 4015 2400
carol.umhoefer@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

GERMANY

Last modified 26 January 2016

LAW IN GERMANY

The main legal source of data protection in Germany is the Federal Data Protection Act (*Bundesdatenschutzgesetz* in German) ("BDSG") which implements the European data protection directive 95/46/EC. Additionally, each German state has a data protection law of its own. In principle, the data protection acts of the individual states intend to protect personal data from processing and use by public authorities of the states whereas the BDSG intends to protect personal data from processing and use by federal public authorities and private bodies. Enforcement is through the data protection authorities of the German states. The competence of the respective state authority depends on the place of business of the data controller.

These will remain the legal sources until the European Data Protection Regulation comes into force in 2018. The Data Protection Regulation will then completely replace the BDSG and the European Data Protection Directive 96/46/EC.

DEFINITIONS

Definition of personal data

The BDSG defines personal data as any information concerning the personal or material circumstances of an identified or identifiable natural person ('data subject').

Definition of sensitive personal data

Sensitive or rather special categories of personal data under the BDSG are any information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.

NATIONAL DATA PROTECTION AUTHORITY

Each individual German state has a Data Protection Authority which is responsible for the enforcement of data protection laws and competent for data controllers established in the relevant state.

REGISTRATION

Unlike most European data protection regimes, German data protection law does not require a registration of automated data processing. In addition, even though the BDSG provides for a notification, such notification is the exception rather than the rule.

This follows from the fact that the notification requirement is waived if the data controller has appointed a data protection officer ('DPO'), which is mandatory for all companies of a certain size (the obligation applies if more than nine persons are regularly involved in the automated processing of personal data). Automated data processing operations with

respect to sensitive data are subject to prior checking by the data controller's internal DPO.

DATA PROTECTION OFFICERS

Data controllers that deploy more than nine persons with the automated processing of personal data are obliged to appoint a DPO. Such a DPO may either be an employee or an external consultant that has sufficient knowledge in the field of data protection. The DPO is neither required to be a citizen nor a resident of Germany, but shall have the necessary expertise in German data protection law as well as reliability.

The DPO shall in particular monitor the proper use of data processing programs and take suitable steps to familiarise the persons employed in the processing of personal data with the provisions of data protection.

As far as sensitive personal data is concerned, such personal data is subject to examination prior to the beginning of processing (prior checking) by the appointed DPO unless the data subject has consented. In case of doubt, the DPO shall liaise with the competent authorities.

Any intentional or negligent infringement of the statutory obligation to appoint a DPO may result in fines up to EUR 50,000. However, the fine shall be higher than the economic advantage gained through the infringement. Therefore, depending on the individual case, the fine may eventually be higher than EUR 50,000.

COLLECTION & PROCESSING

The collection, processing and use of personal data is only admissible if explicitly permitted by the BDSG or any other legal provision or if the data subject has explicitly consented in advance.

In practice, Section 28 BDSG is the most applicable statutory provision permitting collection, processing and use of personal data. For example, Section 28 para. 1 no. 1–3 BDSG provide that the collection, processing or use of personal data as a means of fulfilling one's own business purposes shall be admissible if it is:

- necessary to create, perform or terminate a legal obligation or quasi legal obligation with the data subject
- necessary to safeguard legitimate interests of the controller 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, or
- the personal data is generally accessible or the controller would be allowed to publish them, unless the data subject has a clear and overriding interest.

Sensitive personal data may only be processed if:

- it 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 data involved has manifestly been made public, by the data subject
- it is necessary to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of collection, processing or use, or
- it is necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection, processing and use and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort.

Processing of employee data for employment related purposes is subject to a separate provision (Sec. 32 BDSG) according to which the collection, processing and use of employee data is only permitted regarding decisions on the establishment, implementation and termination of the employment contract.

Whichever of the above conditions is relied upon, upon the first collection of personal data without the data subject's knowledge, the data controller must provide the data subject with 'fair processing information'. This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

With respect to the transfer of personal data to third parties it needs to be differentiated between a transfer within the European Economic Area ("EEA") and a transfer to any other country outside the EEA:

- Due to the harmonisation of data protection law by European law, a transfer of personal data to third parties within the EEA is treated as if it took place within the territory of Germany, ie it is admissible if explicitly permitted by the BDSG or any other legal provision or if the data subject has explicitly consented in advance.
- The transfer of personal data to a country outside the EEA ("cross border") is admissible provided the following conditions are fulfilled:
    - regardless of the fact that the personal data is transferred cross border, a legal basis for the transfer as such is required, ie in the absence of consent, it needs to be explicitly permitted by the BDSG or any other legal provision, and
    - the data recipient needs to ensure an adequate level of data protection. The European Commission considers data recipients in Andorra, Switzerland, Canada, Argentina, Guernsey, the Isle of Man, Faeroe Islands, Israel, New Zealand, Jersey and Uruguay as providing such an adequate level (as of 19 January 2016). In case the data recipient is seated in the US, it should comply with the US Department of Commerce's Safe Harbour Privacy Principles. In addition, adequate safeguards with respect to the protection of personal data can be achieved by entering into binding corporate rules (only applicable if the data recipient is a group company) or by entering into a data processing agreement based on the EU model clauses of the European Commission. Please note that a data transfer agreement based on the EU model clauses must be strictly in compliance with the wording of the model clauses provided by the EU Commission. Please note that in the case of transfers of personal data to the US, until 6 October 2015 the adequate level of data protection was acknowledged as ensured at the recipient if the recipient complied with the US Department of Commerce's Safe Harbour Privacy Principles. Following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU Safe Harbour regime is no longer regarded as a valid basis for transferring personal data to the US.Therefore, currently only binding corporate rules and EU model clauses are sufficient means to ensure an adequate level of data protection at recipients in the US.
- Whether there is a notification requirement, depends on the legal basis for the crossborder transfer. While a transfer based on binding corporate rules always requires involvement of the authorities, a transfer based on Safe Harbour principles or EU model clauses does not. Such transfer is handled differently by the responsible authorities. However, most authorities do not require a notification.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm which might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data.

In the frame of the new IT Security Act, which came into force on 25 July 2015, new provisions have been added to the German Telemedia Act (TMG). According to the TMG service providers, e.g. website operators, have to ensure, as far as technically and economically reasonable, by technical and organizational arrangements, that there is no unauthorized access to their technical facilities and that these are secured against violations of the security of personal data as well as against disorders caused by external attacks. Such arrangements have to be of state of the art technology.

BREACH NOTIFICATION

A breach notification duty has recently been implemented into the BDSG. According to Sec. 42a BDSG the notification duty applies if:

- sensitive personal data, personal data subject to professional secrecy, personal data related to criminal and/or administrative offences, personal data concerning bank or credit card accounts, certain telecommunications and online data is abused or lost and an authorised third party acquires knowledge, and
- in case of telecommunications and online data, there is a serious threat of interference with interests of concerned individuals.

Data controllers are obliged to inform supervisory authorities and the concerned individuals.

ENFORCEMENT

Violation of German data protection laws are subject to pecuniary fines up to EUR 300,000 per violation (administrative offence). In the case of wilful behaviour or if conducted in exchange for a financial benefit (criminal offence), by imprisonment of up to 2 years or a fine depending on how severe the violation is. Authorities may also skim profits generated by data protection breaches.

In the past, German data protection authorities were rather reluctant concerning the enforcement of data protection law, ie very few official prosecution procedures were opened and imposed fines were rather low. However, this has recently changed and we note a tendency to a stricter enforcement. This particularly relates to several data protection scandals involving loss and disclosure or misuse of personal data in the recent years.

Further, reputation damages are usually quite severe if data protection breaches become public. Civil liabilities as well as injunctive reliefs and skimming of profits are likely under the Unfair Competition Act.

ELECTRONIC MARKETING

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the ‘same service/product’ exemption. The exemption concerns marketing emails related to the same products/services as previously purchased from the sender by the user provided:

- the user has been informed of the right to opt-out prior to the first marketing email
- the user did not opt-out, and
- the user is informed of the right to opt-out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communication sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

ONLINE PRIVACY

Traffic data

Traffic data qualifies as personal data. Providers of telecommunication services may collect and use the following traffic data to the following extent:

- the number or other identification of the lines in question or of the terminal
- authorisation codes, additionally the card number when customer cards are used
- location data when mobile handsets are used
- the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted
- the telecommunications service used by the user
- the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted.

Any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Stored traffic data may be used after the termination of a connection only where required to set up a further connection, for billing purposes or in case the user has requested a connection overview.

The service provider may collect and use the customer data and traffic data of subscribers and users in order to detect, locate and eliminate faults and malfunctions in telecommunications systems. This applies also for faults, which can lead to a limitation of availability of information and communications systems or which can lead to an unauthorized access of telecommunications and data processing systems of the users.

Otherwise, traffic data must be erased by the service provider without undue delay following termination of the connection.

Service providers have to inform the users immediately, if any faults of data procession systems of the users become known. Furthermore the service provider has to inform the users about measures for detecting and rectifying faults.

Location Data

Location Data qualifies as personal data. This data may only be processed as required for the provision of requested services and is subject to prior information of the user. For all other purposes, the user's informed consent must be obtained. According to Section 4a BDSG, 13 German Telemdia Act (TMG) this means that:

- the user's consent must be intentional, informed and clear. For this purpose the user must be informed on the type, the scope, the location and the purpose of data collection, processing and use including any forwarding of data to third parties
- the user's consent must be recorded properly
- the user must be able to access the content of his consent declaration any time. It is sufficient that such information is provided upon the users' request
- the user's consent must be revocable at all times with effect for the future.

Users must always be informed on the use of cookies in a privacy notice. Cookies may generally be used if they are required in order to perform the services requested by the user. Otherwise, users must be provided with an opt-out mechanism. For this purpose, information on the use of cookies together with a link on how to adjust browser settings in order to prevent future use is sufficient.

Germany has not yet taken any measures to implement the e privacy directive. However, in February 2014 the German Federal Ministry of Economic declared that the European Commission considers the Cookie Directive as implemented in Germany. However, since the European Commission´s exact interpretation is not known, a final official clarification is awaited. It therefore remains to be seen whether an active opt in, eg by clicking on a pop up screen will be required in the future.

Different rules apply in the case of tracking technologies which collect and store a user's IP address. Since IP addresses qualify as personal data, their processing for tracking and marketing services requires active opt-in consent.

KEY CONTACTS

Thomas Jansen
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +49 89 2323 72 110
thomas.jansen@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

GHANA

Last modified 25 January 2016

LAW IN GHANA

Data Protection Act, 2012 (Act 843) ('Act').

DEFINITIONS

Definition personal data

Personal data is defined as:

- data about an individual who can be identified either:
  - from the data, or
  - from the data and other information in the possession of, or likely to come into the possession of the data controller.

Definition sensitive personal data

The Act does not make provision for 'sensitive personal data'. However 'special personal data', is defined as personal data which relates to:

- a child who is under parental control in accordance with the law, or
- the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behavior of an individual.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commission ('Commission')

Room No. 51
First Floor
Ministry of Communications
Ministerial Enclave
P.O. Box CT 7195
Accra
Ghana

Tel: +233 302 631 455

REGISTRATION

A data controller who intends to process personal data is required to register with the Data Protection Commission. A data controller who is not incorporated in Ghana must register as an external company.

DATA PROTECTION OFFICERS

There is an obligation under the Act for data controllers to appoint data protection officers.

COLLECTION & PROCESSING

A person shall collect data directly from the data subject unless:

- the data is contained in a public record
- the data subject has deliberately made the data public
- the data subject has consented to the collection of the information from another source
- the collection of the data from another source is unlikely to prejudice a legitimate interest of the data subject
- the collection of the data from another source is necessary for a number of expressly designated purposes (for example the detection or punishment of an offence or breach of law)
- compliance would prejudice a lawful purpose for the collection
- compliance is not reasonably practicable.

A data controller must also ensure that the data subject is aware of:

- the nature of the data being collected
- the name and address of the person responsible for the collection
- the purpose for which the data is required for collection
- whether or not the supply of the data by the data subject is discretionary or mandatory
- the consequences of failure to provide the data
- the authorized requirement for the collection of the information or the requirement by law for its collection
- the recipient of the data
- the nature or category of the data
- the existence of the right of access to and the right to request rectification of the data collected before the collection.

Where collection is carried out by a third party on behalf of the data controller, the third party must ensure that the data subject has the information listed above.

TRANSFER

There are no specific provisions in the Act on the transfer of personal data. However, the sale, purchase, knowing or reckless disclosure of personal data or information is prohibited.

A person who knowingly or recklessly discloses personal data is liable on summary conviction to a fine of not more than 250 penalty units or to a term of imprisonment of not more than 2 years or to both. A person who sells or offers for sale personal data is liable on summary conviction to a fine of not more than 2500 penalty units or to a term of imprisonment of not more than five years or to both a fine and a term of imprisonment.

A penalty unit is equivalent to GHS12 (approximately USD $4.00).

SECURITY

A data controller is required to take steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures to prevent:

- loss of, damage to, or unauthorised destruction
- unlawful access to or unauthorised processing of personal data.

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorised person, the data controller or a third party who processes data under the authority of the data controller shall notify the Commission and the data subject of the unauthorised access or acquisition as soon as reasonably practicable after the discovery of the unauthorised access or acquisition of the data. The data controller shall take steps to ensure the restoration of the integrity of the information system.

The data controller shall delay the notification to the data subject where the security agencies or the Data Protection Commission inform the data controller that the notification will impede a criminal investigation.

ENFORCEMENT

Where the Commission is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commission shall serve the data controller with an enforcement notice to require the data controller to do any of the following:

- to take or refrain from taking the steps specified within the time stated in the notice
- to refrain from processing any personal data or personal data of a description specified in the notice
- to refrain from processing personal data or personal data of a description specified in the notice for the purposes specified or in the manner specified after the time specified.

A person who fails to comply with an enforcement notice commits an offence and is liable on summary conviction to a fine of not more than one hundred and fifty penalty units or to a term of imprisonment of not more than one year or to both. A penalty unit is equivalent to GHS12 (approximately USD $4.00).

Further, an individual who suffers damage or distress through the contravention of the data protection obligations by a data controller is entitled to compensation from the data controller for the damage or distress notice.

ELECTRONIC MARKETING

The Act prohibits a data controller from using, obtaining, procuring or providing information related to a data subject for the purpose of direct marketing without the prior written consent of the data subject. However, there are no specific provisions that relate to electronic marketing specifically.

ONLINE PRIVACY

There are no specific provisions in relation to on-line privacy. However, a data controller is generally required to take necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of

appropriate, reasonable, technical and organizational measures.

KEY CONTACTS

Reindorf Chambers
www.reindorfchambers.com

Kizzita Mensah
T +233 302 225674/ 249564
kizzita.mensah@reindorfchambers.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

GIBRALTAR

Last modified 24 January 2015

LAW IN GIBRALTAR

A territory within the European Union (by virtue of the accession of the United Kingdom on 1 January 1973) Gibraltar implemented the EU data Protection directive 95/46 EC in 2006 with the Data Protection Act 2004 (‘Act’). Enforcement is through the offices of the Data Protection Commissioner ('DPC').

DEFINITIONS

Definition of personal data

Any information relating to a Data Subject; and a Data Subject means a natural person who is the subject of Personal Data.

Definition of sensitive personal data

Information about racial or ethnic origin, religious or philosophical beliefs, trade union membership, health or sex life. The definition includes data regarding the commission or alleged commission of any offence and information on any proceedings for offences or alleged offences, the disposal of such proceedings and any sentence given.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commissioner

Gibraltar Regulatory Authority
Suite 603 Europort
Gibraltar

T 200 74636
F 200 72166

info@gra.gi

REGISTRATION

Data controllers who process personal data must notify the Data Protection Commissioner by registering with the Gibraltar Regulatory Authority (‘GRA’) so that their processing of personal data may be registered and made public in the Data Protection Register, unless an exemption applies. Once registered any changes to the processing of personal data will require the Data Protection Register to be updated.

The notification must contain the following information:

- name and address of data controller and any representative
- description of the personal data being processed and the Categories to which they relate
- description of the purpose of the processing
- description of the recipients or categories of recipient to whom data will be sent
- names of any countries outside the EEA to which data is to be transferred to
- an adequate description of the security measures taken that is sufficient to allow a preliminary assessment of those measures, and
- other information reasonably required by the DPC.

DATA PROTECTION OFFICERS

There is no requirement in Gibraltar for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject has unambiguously given his consent
- the processing is necessary for the performance of a contract to which the data subject is a party, or for actions to be carried out at the request of the data subject prior to entering into a contract
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject
- the processing is necessary to prevent:
    - injury or other damage to the health of the data subject
    - serious loss or damage to his property
    - to protect his vital interests where seeking consent is likely to damage those interests
- the processing is necessary for a public purpose, namely:
    - for the administration of justice
    - for the performance of a statutory function
    - for the performance of a function of Government or of a Government Minister
    - the processing is necessary for the performance of a public function carried out in the public interest, and
    - the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplied, except where the rights of the data subject under the European Convention of Human Rights and the Gibraltar Constitution prevail.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more

stringent conditions.

TRANSFER

Data controllers may transfer personal data out of the EEA if any of the following conditions are met:

- the country to which the data is being transferred ensures an adequate level of protection by reference to statutory parameters
- the data subject consents to the transfer
- the transfer is necessary:
    - to perform a contract between the data subject and the data controller
    - to take steps at the request of the data subject in order to enter into a contract with the data controller
    - for the agreement or performance of a contract between a third party and the data controller at the request of the data subject
    - the transfer of data is required pursuant to an international obligation of Gibraltar; – the transfer is necessary due to a substantial public interest
    - the transfer is necessary to obtain legal advice either in respect of proceedings or to establish or defend a legal right
    - the transfer is necessary to protect the vital interests of the data subject, and
    - the transfer is made as part of personal data stored on a public register.

If none of these conditions are met, data outside of the EEA may still be transferred if:

- it is to a country approved by the EU commission as safe
- it is to a US organisation falling within the Safe Harbour provisions, or
- on terms incorporating the Model Clauses or approved Corporate Binding Rules. Alternatively the data controller can apply to the DPC for specific approval on a case by case basis.

SECURITY

Data controllers must take appropriate technical and organisational measures against accidental or unlawful destruction, loss or alteration of data, or against unauthorised disclosure or access to the information, and generally against all other unlawful forms of processing.

BREACH NOTIFICATION

There is currently no mandatory requirement in the Act to report data security breaches or losses to the DPC or to data subjects. A mandatory requirement will be introduced with the transposition into Gibraltar law of the Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications) introduced by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

ENFORCEMENT

In Gibraltar, the DPC is responsible for the enforcement of the Act. If he becomes aware that the data controller is in breach of the Act, he can initiate proceedings against the data controller.

The ultimate sanction on conviction for an offence is a fine of GBP 4,000 (in the case of summary conviction in the magistrate's court) or GBP 10,000 (in the case of indictment in the Supreme Court).

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (eg a right to 'opt out') for direct marketing purposes.

The Communications (PD&P) Regulations 2006 ('the Regulations') prohibit the use of automated calling systems without the consent of the recipient and unsolicited emails can only be sent without consent if:

- the contact details have been provided in the course of a sale or negotiations
- the marketing relates to a similar product or services, and
- the recipient was given a means of refusing the use of their contact details for marketing when they were collected.

Direct marketing emails must not disguise or conceal the identity of the sender in contravention of the E-Commerce Act. SMS marketing is also likely to be included within the prohibition on email marketing.

The restrictions on marketing by email only apply in relation to individuals and not where email marketing is sent to corporations.

ONLINE PRIVACY

The Regulations deal with the collection of location and traffic data by public electronic communications providers ('CPs') and the use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- it is being used to provide a value added service, and
- consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CP for:

- the management of billing or traffic
- dealing with customer enquiries
- the prevention of fraud
- the marketing of electronic communications services, or
- the provision of a value added service.

Location Data

Location Data may only be processed for the provision of value added services with consent and where the identity of the user is anonymised. CPs are also required to take measures and put a policy in place to ensure the security of the personal data they process.

Cookie Compliance

The use and storage of cookies and similar technologies requires:

- clear and comprehensive information, and
- consent of the website user.

Usual data protection principals of the Act also apply. Consent is not required for cookies that are used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or where this is strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the Regulations is dealt with by the DPC and if found guilty a fine and or imprisonment may be imposed. However an individual may also bring an action for damages in the Supreme Court.

KEY CONTACTS

Hassans
www.gibraltarlaw.com/

Michael Nahon
Partner
T (+350) 200 79000
michael.nahon@hassans.gi

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

GREECE

Last modified 21 January 2016

LAW IN GREECE

Greece implemented the EU Data Protection Directive 95/46/EC in October 1997 by Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data, as amended ('Law'). Such law is currently in force as amended by Laws 3471/2006, 3783/2009, 3947/2011, 4024/2011 and 4070/2012, and 4139/2013.

Enforcement is through the Data Protection Authority ('DPA').

DEFINITIONS

Definition of personal data

'Personal data' shall mean any information relating to the data subject. Personal data is not considered to be the consolidated data of a statistical nature where data subjects may no longer be identified.

Definition of sensitive personal data

'Sensitive data' shall mean the data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, social welfare and sex life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Authority

1-3 Kifissias Avenue, Athens, Greece.
T 2106475600
F 2106475628

contact@dpa.gr

The DPA is responsible for overseeing the Data Protection Law.

REGISTRATION

The data controller must notify the DPA in writing about the establishment and operation of a file or the commencement of data processing. In the course of the aforementioned notification, the data controller must necessarily declare the following:

- His/her name, trade name or distinctive title, as well as his/her address

- The address where the file or the main hardware supporting the data processing is established
- The description of the purpose of the processing of personal data included or about to be included in the file
- The category of personal data that is being processed or about to be processed or included or about to be included in the file
- The time period during which s/he intends to carry out data processing or preserve the file
- The recipients or the categories of recipients to whom such personal data is or may be communicated
- Any transfer and the purpose of such transfer of personal data to third countries
- The basic characteristics of the system and the safety measures taken for the protection of the file or data processing.

The above data is then registered with the Files and Data Processing Register kept by the DPA. Any modification of the above data must be communicated in writing and without any undue delay by the data controller to the DPA.

DATA PROTECTION OFFICERS

There is no requirement in Greece for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Processing personal data

Collection and processing of personal data is permitted only when the data subject has given his/her consent. Exceptionally, data may be processed even without such consent, but only if:

- processing is necessary for the execution of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for the compliance with a legal obligation to which the data controller is subject
- processing is necessary in order to protect the vital interests of the data subject, if s/he is physically or legally incapable of giving his/her consent
- processing is necessary for the performance of a task carried out in the public interest or a project carried out in the exercise of public function by a public authority or assigned by it to the data controller or a third party to whom such data are communicated
- processing is absolutely necessary for the purposes of a legitimate interest pursued by the data controller or a third party or third parties to whom the data is communicated and on condition that such a legitimate interest evidently prevails over the rights and interests of the persons to whom the data refer and that their fundamental freedoms are not affected

Processing sensitive personal data

The collection and processing of sensitive data is prohibited. Exceptionally, the collection and processing of sensitive data, as well as the establishment and operation of the relevant file, is permitted by the DPA, when one or more of the following conditions occur:

- the data subject has given his/her written consent, unless such consent has been extracted in a manner contrary to the law or bonos mores or if the law provides that any consent given may not lift the relevant prohibition
- processing is necessary to protect the vital interests of the data subject or the interests provided for by the law of

a third party, if s/he is physically or legally incapable of giving his/ her consent

- processing relates to data made public by the data subject or is necessary for the recognition, exercise or defence of rights in a court of justice or before a disciplinary body
- processing relates to health matters and is carried out by a health professional subject to the obligation of professional secrecy or relevant codes of conduct, provided that such processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services
- processing is carried out by a Public Authority and is necessary for the purposes of:
  - national security
  - criminal or correctional policy and pertains to the detection of offences, criminal convictions or security measures
  - protection of public health, or
  - the exercise of public control on fiscal or social services
- processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained and all necessary measures for the protection of the persons involved are taken, or
- processing concerns data pertaining to public figures, provided that such data are in connection with the holding of apublic office or the management of third parties' interests, and is carried out solely for journalistic purposes. The DPA may grant a permit only if such processing is absolutely necessary in order to ensure the right to information on matters of public interest, as well as within the framework of literary expression and provided that the right to protection of private and family life is not violated in any way whatsoever.

The DPA grants a permit for the collection and processing of sensitive data, as well as a permit for the establishment and operation of the relevant file, upon request of the data controller.

The permit is issued for a specific period of time, depending on the purpose of the data processing. It may be renewed upon request of the data controller.

The permit must necessarily contain the following:

- the full name or trade name or distinctive title, as well as the address, of the data controller and his/her representative, if any
- the address of the place where the file is established
- the categories of personal data which are allowed to be included in the file
- the time period for which the permit is granted
- the terms and conditions, if any, imposed by the DPA for the establishment and operation of the file, and
- the obligation to disclose the recipient or recipients as soon as they are identified.

A copy of the permit is registered with the Permits Register kept by the DPA. Any change in the above data must be communicated without undue delay to the DPA. Any change other than a change of address of the data controller or his/her representative must entail the issuance of a new permit, provided that the terms and conditions stipulated by law are fulfilled.

TRANSFER

The transfer of personal data is permitted:

- for member states of the European Union

- for a non member of the European Union following a permit granted by the DPA if it deems that the country in question guarantees an adequate level of protection. For this purpose it shall particularly take into account the nature of the data, the purpose and the duration of the processing, the relevant general and particular rules of law, the codes of conduct, the security measures for the protection of personal data, as well as the protection level in the countries of origin, transit and final destination of the data. A permit by the DPA is not required if the European Commission has decided, on the basis of the process of article 31, paragraph 2 of Directive 95/46/EC of the Parliament and the Council of 24 October 1995, that the country in question guarantees an adequate level of protection, in the sense of article 25 of the aforementioned Directive.

The transfer of personal data to a non member state of the European Union which does not ensure an adequate level of protection is exceptionally allowed only following a permit granted by the DPA, provided that one or more of the following conditions occur:

- the data subject has consented to such transfer, unless such consent has been extracted in a manner contrary to the law or bonos mores

- the transfer is necessary:
    - in order to protect the vital interests of the data subject, provided s/he is physically or legally incapable of giving his/her consent

    - for the conclusion and performance of a contract between the data subject and the data controller or between the data controller and a third party in the interest of the data subject, if he/she is incapable of giving his/her consent, or

    - for the implementation of pre contractual measures taken in response to the data subject's request

- the transfer is necessary in order to address an exceptional need and safeguard a superior public interest, especially for the performance of a co operation agreement with the public authorities of the other country, provided that the data controller provides adequate safeguards with respect to the protection of privacy and fundamental liberties and the exercise of the corresponding rights

- the transfer is necessary for the establishment, exercise or defence of a right in court

- the transfer is made from a public register which by law is intended to provide information to the public and which is accessible by the public or by any person who can demonstrate a legitimate interest, provided that the conditions set out by law for access to such register are in each particular case fulfilled, or

- the data controller shall provide adequate safeguards with respect to the protection of the data subjects' personal data and the exercise of their rights, when the safeguards arise from conventional clauses which are in accordance with the regulations of the Law. A permit is not required: in the case of the Standard Contractual Clauses approved by the European Commission; and in cases where the Binding Corporate Rules have been executed. Please note that prior to the issuance of the Judgment of the European Union Court of Justice dated October 6th, 2015 in the Schrems case (C-362/14), the US-EU safe harbor regime was also regarded by the DPA as a valid basis for transferring personal data to the US. Upon recent developments though, transfers of data to the U.S.A. are currently subject to the DPA's authorization (unless they take place on the basis of the EC Standard Model Clauses).

SECURITY

The processing of personal data must be confidential. It must be carried out solely and exclusively by persons acting under the authority of the data controller or the processor and upon his/her instructions.
In order to carry out data processing the data controller must choose persons with corresponding professional qualifications providing sufficient guarantees in respect of technical expertise and personal integrity to ensure such confidentiality.

The data controller must implement appropriate organisational and technical measures to secure data and protect it against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data subject to processing.

If the data processing is carried out on behalf of the data controller, by a person not dependent upon him, the relevant assignment must necessarily be in writing. Such assignment must necessarily provide that the processor carries out such data processing only on instructions from the data controller and that all other confidentiality obligations must *mutatis mutandis* be borne by him.

BREACH NOTIFICATION

There is no mandatory requirement in the Law to report data security breaches or losses to the DPA or to data subjects.

ENFORCEMENT

The DPA may impose on the data controllers or on their representatives, if any, the following administrative sanctions for breach of their duties arising from the Law as well as from any other regulation on the protection of individuals from the processing of personal data:

- a warning with an order for the violation to cease within a specified time limit
- a fine amounting between EUR 880 and EUR 147,000
- a temporary revocation of the permit
- a definitive revocation of the permit, or
- the destruction of the file or a ban on the processing and the destruction, return or locking of the relevant data.

In addition the following penal sanctions may be imposed:

- anyone who fails to notify the DPA of the establishment or the operation of a file or any change in the terms and conditions regarding the granting of the permit will be punished by imprisonment for up to three years and a fine amounting between EUR 2,940 and EUR 14,705
- anyone who keeps a file without permit or in breach of the terms and conditions referred to in the DPA's permit, will be punished by imprisonment for a period of at least one year and a fine amounting between EUR 2,940 and EUR 14,705
- anyone who proceeds to the interconnection of files without notifying the DPA accordingly will be punished by imprisonment for up to three years and a fine amounting between EUR 2,940 and EUR 14,705. Anyone who proceeds to the interconnection of files without the DPA's permit, wherever such permit is required, or in breach of the terms of the permit granted to him, will be punished by imprisonment for a period of at least one year and a fine amounting between EUR 2,940 and EUR 14,705
- anyone who unlawfully interferes in any way whatsoever with a personal data file or takes notice of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to

unauthorised persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment and a fine and, regarding sensitive data, by imprisonment for a period of at least one year and a fine amounting between EUR 2,940 Euros and EUR 29,411, unless otherwise subject to more serious sanctions

- any data controller who does not comply with decisions issued by the DPA in the exercise of the right of access, in the exercise of the right to object, as well as with acts imposing the administrative sanctions will be punished by imprisonment for a period of at least two years and a fine amounting between EUR 2,940 and EUR 14,705. The sanctions referred to in the preceding sentence will also apply to any data controller who transfers personal data, in breach of the Law

- if the data controller is not a natural person, then the representative(s) of the legal entity shall be liable, and

- finally, any natural person or legal entity of private law, who in breach of the Law, causes material damage will be liable for damages in full. If the same causes non pecuniary damage, s/he will be liable for compensation. Liability subsists even when said person or entity should have known that such damage could be brought about. The compensation payable according to article 932 of the Civil Code for non-pecuniary damage caused in breach of the Law has been set at the amount of at least EUR 5,882, unless the plaintiff claims a lesser amount or the said breach was due to negligence. Such compensation shall be awarded irrespective of the claim for damages.

ELECTRONIC MARKETING

Electronic marketing is regulated by Law 3471/2006 'for the protection of personal data and privacy in electronic communications' (the 'Law'), in combination with the general provisions of Law 2472/1997 *'for the protection of individuals from the processing of personal data'* (the 'Data Protection Act').

According to the provisions of article 11 of the Law, data processing for electronic marketing purposes is allowed only upon the individuals' prior express consent. The said article prohibits the use of automated calling systems for marketing purposes to subscribers that have previously declared to the public electronic communications services providers ('CSPs') that they do not wish to receive such calls in general. The CSPs must register these declarations for free on a separate publicly accessible list.

Personal data (such as e-mail addresses) that have been legally obtained in the course of sales of products, provision of services or any other transaction may be used for electronic marketing purposes, without the receiver's prior consent thereto, provided that the receiver of such email has the possibility to 'opt out' for free to the collection and processing of his/ her personal data for the aforementioned purposes.

Direct marketing emails or advertising emails of any kind are absolutely prohibited, when the identity of the sender is disguised or concealed and also when no valid address, to which the receivers can address requests for the termination of such communications, is provided.

ONLINE PRIVACY

Articles 4 and 6 of the Law (as amended by Directive 2009/136/EC) deals with the collection of location and traffic data by CSPs and the use of cookies and similar technologies.

Traffic data

Traffic data of subscribers or users held by a CSP must be erased or anonymised after the termination of a communication, unless they are retained for one the following reasons:

- The billing of subscribers and the payment of interconnections, provided that the subscribers are informed of the categories of traffic data that are being processed and the duration of processing, which must not exceed 12

months from the date of the communication (unless the bill is doubtable or unpaid).

- Marketing of electronic communications services or value added services, to the extent that traffic data processing is absolutely necessary and following the subscriber's or the user's prior express consent thereto, after his/her notification regarding the categories of traffic data that are being processed and the duration of the processing. Such consent may be freely recalled. The provision of electronic communication services by the CSP must not depend on the subscriber's consent to the processing of his/her traffic data for other purposes (eg. Marketing purposes).

Location data

Location data may only be processed for the provision of value added services, only if such data are anonymised or with the subscriber's/ user's express consent, to the extent and for the duration for which such processing is absolutely necessary. The CSP must previously notify the user or the subscriber of the categories of location data that are being processed, the purposes and the duration of the processing as well as of the third parties to which the data will be transmitted for value added services provision. The subscriber's/user's consent may be freely recalled and the 'opt out' possibility must be provided to the subscriber by the CSP free of charge and with simple means, every time he is connected to the network or in each transmission of communication.

Location data processing is allowed exceptionally without the subscriber's/user's prior consent to authorities dealing with emergencies, such as prosecution authorities, first aid or fire-brigade authorities, when the location of the caller is necessary for serving such emergency purposes.

Cookie compliance

The use and storage of cookies and similar technologies is allowed when the subscriber/user has provided his express consent, after his/her comprehensive and detailed notification by the CSP. The subscriber's consent may be provided through the necessary browser adjustments or through the use of other applications.

The latter do not prevent the technical storage or use of cookies for purposes relating exclusively to the transmission of a communication through an electronic communications network or the provision of an information society service for which the subscriber or the user has specifically requested. The Data Protection Authority is the competent authority for the issuance of an Act, which will regulate the ways such services will be provided and the subscribers' consent will be declared.

KEY CONTACTS

Kyriakides Georgopoulos Law Firm
www.kglawfirm.gr

Effie Mitsopoulou
Partner
T +30 210 817 1540
e.mitsopoulou@kglawfirm.gr

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

GUERNSEY

Last modified 27 January 2016

LAW IN GUERNSEY

The processing of personal data in Guernsey is regulated by the Data Protection (Bailiwick of Guernsey) Law 2001 as amended (the 'Law').

Guernsey has been recognised by the European Commission as providing an adequate level of protection for personal data for the purposes of the Eighth Data Protection Principle (see European Commission Directive 2003/821/EC).

Enforcement of the law is through the Data Protection Commissioner (the 'Commissioner'), an independent public official appointed by the States of Guernsey.

DEFINITIONS

Definition of personal data

Under the Law, 'personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Definition of sensitive personal data

'Sensitive personal data' means personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a labour organisation, such as a trade union
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, and
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Office

Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0) 1481 742074
F: +44 (0) 1481 742077
W: www.dataci.gg

http://www.gov.gg/DataProtection

REGISTRATION

Personal data must not (except in limited circumstances) be processed unless the data controller is registered with the Commissioner. Any data controller who wishes to be included in the register must provide a notification to the Commissioner (an online portal is available). Such a notification must specify:

1. the name and address of the data controller
2. the name and address of any nominated representatives
3. a description of the data and the category or categories of data subject to which they relate
4. why the information is processed
5. a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data, and
6. the names, or a description of, any countries or territories outside the Bailiwick of Guernsey to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data.

The notification must also contain a general description of the measures to be taken to prevent unauthorised or unlawful processing of, accidental loss or destruction of, or damage to, personal data.

The data controller is required to notify the Commissioner of any changes to the registered details.

DATA PROTECTION OFFICERS

There is no statutory requirement to have a data protection officer. However, where a data controller is not established in the Bailiwick but uses equipment in the Bailiwick for processing the data (otherwise than for the purposes of transit through the Bailiwick), the data controller must nominate a representative who is established in the Bailiwick. If such a representative is nominated, then their name and address forms part of the registrable particulars as detailed in the section above.

COLLECTION & PROCESSING

Data controllers may process personal data when any of the following conditions are met:

- the data subject consents
- 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 data subject's request with a view to entering into a contract
- the processing is necessary for compliance with the data controller's legal obligations, other than an obligation imposed by contract
- the processing is necessary in order to protect the vital interests of the data subject, or
- the processing is necessary for the administration of justice, the exercise of a function in the public interest or the exercise of official authority.

Where sensitive personal data is processed one of a further list of more stringent conditions must also be met.

TRANSFER

Personal data must not be transferred to a country or territory outside of the Bailiwick of Guernsey unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The exceptions to that principle are as follows:

- the data subject has given consent to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the data controller or for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller
- the transfer is necessary for the conclusion of a contract between the data controller and a person other than the data subject which is entered into at the request of the data subject or is in the interests of the data subject, or is necessary for the performance of such a contract
- the transfer is necessary for reasons of substantial public interest
- the transfer is necessary for, or in connection with, legal proceedings, obtaining legal advice or for the purposes of establishing, exercising or defending legal rights
- the transfer is necessary to protect the vital interests of the data subject
- the transfer is part of personal data on a public register
- the transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects
- the transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of the data subject.

The Commissioner has published a guidance note entitled 'Exporting Data' which sets out the following approved methods of exporting personal data:

- within the EEA without restrictions
- to another country or territory recognised by a European Commission Decision as ensuring adequate protection
- to entities located in the USA and adhering to the Safe Harbor Privacy Principles
- within a multi-national corporation by using Binding Corporate Rules, which are to be agreed between the exporter and the relevant national Data Protection Authority, or
- to non-EU countries, provided that the transfer is made using the approved EU or (more recommended) the International Chamber of Commerce Contractual Clauses,
- provided always that the Data Protection Principles (as set out in the Law) are complied with.

Following the decision of the Court of Justice of the European Union in Schrems v Data Protection Commissioner (C36214), the US/EU "Safe Harbour" regime is no longer regarded as a valid basis for transferring personal data to the US. Whilst Guernsey is not a member of the EU, it can (and does) adopt measures prescribed by the EU in certain areas such as data protection. Guernsey uses the EU "adequacy" benchmark to assess whether transfers can be validly made to other jurisdictions.

The Safe Harbour regime had been relied upon as a mechanism for the transfer of data to the US, which did not otherwise have "adequate" measures in place to protect personal data. Now that the regime has been abolished, Guernsey businesses are reviewing their procedures. Whilst the Commissioner has not adopted any formal stance in response to the Schrems decision, she is maintaining a close dialogue with the Channel Islands' Brussels office and the UK's Information Commissioner's Office. Whilst awaiting the revised version of the Safe Harbour Privacy Principles, the Commissioner has confirmed that Guernsey's existing statutory regime will be adhered to, confirming that she retains the power to investigate complaints made to her, including those founded on transfers reliant upon Safe Harbour as a basis for their validity.

It is anticipated that the Commissioner will likely await the outcome of the US/EU negotiations, however with the prospect of data protection authorities around Europe adopting varying stances, the immediate future remains uncertain. It remains important for businesses to review their procedures and adopt alternative mechanisms if they had previously relied on Safe Harbour.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data.

Having regard to the state of technological development and the cost of implementing any measures, the measures required must ensure a level of security appropriate to:

1. the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage to, personal data, and
2. the nature of the data to be protected.

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must:

1. choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
2. take reasonable steps to ensure compliance with those measures.

BREACH NOTIFICATION

There is no mandatory requirement in the law to report data security breaches or losses to the Commissioner or to data subjects.

However, under the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance 2004, a provider of a public electronic communications service (the 'service provider') is required to notify subscribers of a significant risk to the security of the service.

ENFORCEMENT

The Commissioner is responsible for the enforcement of the Law.

If the Commissioner is satisfied that a data controller has contravened or is contravening any of the Data Protection Principles, the Commissioner may serve them with a notice ('Enforcement Notice') requiring them, to do either or both of the following:

1. to take, or to refrain from taking, such steps as may be specified. or
2. to refrain from processing personal data.

In certain circumstances the Commissioner may serve on the data controller or the data processor a notice requiring the data controller or data processor to provide specified information to him ('Information Notice').

The Commissioner may decide to issue an Information Notice as a result of:

1. a request received by or on behalf of any person who is, or believes themselves to be, directly affected by any processing of personal data, or
2. the Commissioner reasonably requires the information for determining whether a data controller has complied or is complying with the Data Protection Principles.

Failure to comply with an Enforcement Notice or Information Notice is a criminal offence and can be punished:-

1. on summary conviction, by way of a fine not exceeding £10,000, or
2. on conviction on indictment, by way of an unlimited fine.

The Law also contains provisions for imprisonment and/or an unlimited fine in the event of a person being guilty of an offence of knowingly or recklessly obtaining, or disclosing personal data, without the consent of the data controller.

ELECTRONIC MARKETING

Direct marketing by electronic means to individuals and organisations is regulated by the European Communities (Implementation of Privacy) Directive (Guernsey) Ordinance 2004 (the 'Ordinance'). The Law will also likely have an impact, as there is likely to be processing and use of personal data. The Law does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (ie a right to 'opt out') for direct marketing purposes.

The Ordinance prohibits the use of automated calling systems without the consent of the recipient. Unsolicited emails can only be sent without consent if:

- the contact details have been provided in the course of a sale or negotiations for a sale
- the marketing relates to a similar product or service, and
- the recipient was given a simple method of refusing the use of their contact details when they were collected.

The identity of the sender cannot be concealed in direct marketing communications sent electronically (which is likely to include SMS marketing).

These restrictions only apply in respect of individuals and not where corporations are sent marketing communications.

ONLINE PRIVACY

The 2011 amendments implemented by the UK in relation to cookies have not found their way into Guernsey law and there are no immediate plans for this to be done. However, certain aspects of online privacy nevertheless remain governed by the Ordinance (*defined in Electronic Marketing above)*.

As a matter of good practice, the use of cookies should be identified to web users and they should be allowed to “opt out” of their use if they so wish.

Traffic data held by a service provider must be erased or anonymised when it is no longer necessary for the purpose of a transmission or communication. Exceptions include if the information is being retained in order to provide a value added service to the data subject or if it is held with their consent.

Traffic data should only be processed by a service provider for (a) the management of billing or traffic, (b) customer enquiries, (c) the prevention or detection of fraud, (d) the marketing of electronic communications services, or (e) the provision of a value added service.

Location data may only be processed where the user/subscriber cannot be identified from that data or for the provision of a value added service with consent.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Richard Field
Counsel
T +44 1481 72 72 72
richard.field@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

HONDURAS

Last modified 24 January 2015

LAW IN HONDURAS

Personal Data Protection is regulated mainly in:

- *National Constitution*: Article 182 provides the constitutional protection of Habeas Data, giving individuals the right 'to access any file or record, private or public, electronic or hand written, that contains information which may produce damage to personal honour and family privacy. It is also a method to prevent the transmission or disclosure of such data, rectify inaccurate or misleading data, update data, require confidentiality and to eliminate false information. This guarantee does not affect the secrecy of journalistic sources.'

- *Law of the Civil Registry* (Article 109, Decree 62-2004). This Law refers only to public personal information that is contained in the archives of the Civil Registry.

- *Law for Transparency and for Access to Public Information* (Article 3.5, Decree 170-2006). This law enables the access of any person to all the information contained in public entities, except that which is classified as 'Confidential.' It also extends the Constitutional Protection of Habeas Data and forbids the transmission of personal information that may cause any kind of discrimination or any moral or economic damage to people.

- *Rulings on the Law for Transparency and for Access to Public Information* (Article 42, Accord 001-2008). Provide a definition of databases containing personal confidential information, and requires data subject consent, prior to the use of it by any third party.

In addition, a Law for Data Privacy Protection and Habeas Data is being discussed in the Honduran Congress. It is expected to be approved during the first congressional session of 2015.

DEFINITIONS

Definition of personal data

'Public Personal Data' under the *Law of the Civil Registry* is: 'Public Data' whose disclosure is not restricted in any way, and includes the following:

- names and surnames
- ID number
- date of birth and date of death
- gender
- domicile (but not address)
- job or occupation
- nationality, and

- civil status

Definition of sensitive personal data

'Sensitive Personal Data' in the *Law for Transparency and for Access to Public Information* is defined as: *'Those personal data relating to ethnic or racial origin, physical, moral or emotional characteristics, home address, telephone number, personal electronic address, political participation and ideology, religious or philosophical beliefs, health, physical or mental status, personal and familiar heritage and any other information related to the honour, personal or family privacy, and self-image.'*

Other Definitions:

- *Consent*: Written and express authorisation of the person to whom the personal data refers in order to disclose, distribute, commercialise, and/or use it in a different way as it was originally given for.

- *Confidential Information*: Information provided by particular persons to the Government which is declared confidential by any law, including sealed bids for public tenders.

- *Classified Information*: Public information classified as that by the law, and/or by resolutions issued by governmental institutions.

NATIONAL DATA PROTECTION AUTHORITY

Two entities are responsible for enforcing personal data protection:

1. National Civil Registry
   http://www.rnp.hn

2. Institute for the Access to Public Information
   http://www.iaip.gob.hn

REGISTRATION

Only 'Obligated Entities' must inform the Institute for the Access to Public Information of their databases. Obligated Entities are:

- government institutions
- NGO's
- entities that receive public funds, and
- trade unions with tax exemptions

The Institute for the Access to Public Information will maintain a list of the databases of the above-mentioned entities.

DATA PROTECTION OFFICERS

Only Obligated Entities must appoint a data protection officer.

COLLECTION & PROCESSING

Individuals, companies, and/or Obligated Entities that collect personal data may not use sensitive personal data or confidential information without the consent of the person to whom such information relates.

However, consent is not required to use or transfer personal data in the following cases:

- if the information is used for statistical or scientific needs, but only if the personal data is provided in a way that it cannot be associated with the individual to whom it relates

- if the information is transmitted between Obligated Entities, only if the data is used in furtherance of the authorised functions of those entities
- If ordered by a Court
- If the data is needed for the purpose it was provided to the individual or company to perform a service. Such third parties may not use personal information for purposes other than those for which it was transferred to them, and
- In other cases established by law.

TRANSFER

Individuals and/or companies may not transfer, commercialise, sell, distribute or provide access to personal data contained in databases developed in the course of their job, except with the express and direct written consent of the person to whom that data refers, subject to the exceptions set forth above.

SECURITY

The Institute for the Access to Public Information has the authority to enforce all Obligated Entities to take necessary security measures for the protection of the personal data they collect and/or use.

The Law neither clarifies nor specifically identifies the security policies or security mechanisms that Obligated Entities must comply with.

As a general statement, the Institute for the Access to Public Information has to ensure the security of all Public Information, of all information classified as confidential by public entities, of all sensitive personal data, and of all information to which the Law gives a secrecy status.

BREACH NOTIFICATION

Breach notification is not required.

ENFORCEMENT

The Institute for the Access to Public Information may receive complaints of abuses regarding the collection of personal or confidential data.

The Institute will impose corrective measures and establish recommendations for those persons or companies who disclose personal data, Sensitive Personal Data or confidential data without authorisation.

ELECTRONIC MARKETING

There is no law or regulation that specifically regulates electronic marketing.

ONLINE PRIVACY

There is no law or regulation that specifically regulates online privacy.

KEY CONTACTS

Bufete Gutiérrez Falla y Asociados
www.gufalaw.com/

Julio Alejandro Pohl Garcia Prieto
Associate
T +504 2238-2455
julio.pohl@gufalaw.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

HONG KONG

Last modified 27 January 2016

LAW IN HONG KONG

The Personal Data (Privacy) Ordinance (Cap. 486) ('Ordinance') regulates the collection and handling of personal data. Enforcement is through the Office of the Privacy Commissioner for Personal Data ('PCPD').

The Ordinance was significantly amended by the Personal Data (Privacy) (Amendment) Bill ('Bill') in July 2012. Most of the amendments introduced by the Bill came into force on 1 October 2012. Two major areas of amendments, namely new restrictions against the use and provision of personal data in direct marketing and new powers of the PCPD to provide legal assistance to persons in civil proceedings have also come into force on 1 April 2013.

DEFINITIONS

Definition of personal data

'Personal Data' is defined in the Ordinance as any data:

- relating directly or indirectly to a living individual
- from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and
- in a form in which access to or processing of the data is practicable.

Definition of sensitive personal data

The concept of sensitive personal data does not apply in Hong Kong.

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Privacy Commissioner for Personal Data 12/F, 248

Queen's Road East
Wanchai
Hong Kong

T +852 2827 2827
F +852 2877 7026

http://www.pcpd.org.hk/

The PCPD is responsible for overseeing compliance with the Ordinance.

REGISTRATION

Currently, there is no requirement for the registration of data users in Hong Kong.

However, under the Ordinance the PCPD has the power to specify certain classes of data users to whom registration and reporting obligations apply. Under the Data User Return Scheme ('DURS'), data users belonging to the specified classes are required to submit data returns containing prescribed information to the PCPD, which will compile them into a central register accessible by the public. However, at the time of writing, no register has been created to date. The PCPD has proposed to implement the DURS in phases, with the initial phase covering data users from the following sectors and industries:

- the public sector
- banking, insurance and telecommunications industries, and
- organisations with a large database of members (eg customer loyalty schemes).

A public consultation for the DURS by the PCPD was concluded in September 2011. The PCPD had originally planned to implement the DURS in the second half of 2013. However, in January 2014, the PCPD indicated that it planned to put the DURS on hold until the reforms of the European Union data protection system have been finalised (as the Hong Kong model is based on the same) but no exact time-frame for the implementation has been announced.

DATA PROTECTION OFFICERS

Currently, there is no legal requirement for data users to appoint a data protection officer in Hong Kong. However the PCPD issued a best practice guide in February 2014 to advocate the development of a privacy management programme and encourage data users to appoint or designate a responsible person to oversee the data users' compliance with the Ordinance. This role may or may not be a full-time job, and there is no specific requirement for a Hong Kong citizen or resident to hold this role. There is no particular enforcement action or penalty if a company does not appoint a data protection officer.

COLLECTION & PROCESSING

A data user may collect personal data from data subjects if:

- the personal data is related to a function of the data user
- the collection is necessary, lawful and fair
- the data collected is not excessive, and
- the data user has been informed of the following:
    - whether the provision of personal data by data subjects is mandatory and the consequence(s) for not supplying the data
    - the purposes for which the data will be used
    - the persons to whom the data may be transferred
    - the data subjects' right to request for access and/or correction their personal data, and
    - the contact details of the person to whom requests for access or correction should be sent.

Data users may only use and process personal data for purposes for which the data was collected. Any usage of personal data for new purposes requires the prescribed consent of the data subject concerned.

TRANSFER

Data users may not transfer personal data to third parties, unless the data subjects have been informed of the following before their personal data was collected:

- that their personal data may be transferred
- the classes of persons to whom the data may be transferred.

There are currently no restrictions for transfer of personal data outside of Hong Kong. However, cross-border transfer restrictions are set out in the Ordinance and are expected to come into force in the near future. When these restrictions come into force, they will have a significant impact upon outsourcing arrangements, intra group data sharing arrangements, compliance with overseas reporting obligations and other activities that involve cross border data transfer.

SECURITY

Data users are required by the Ordinance to take all practicable steps to protect personal data against unauthorised or accidental access or loss. The steps which are considered appropriate depend on the nature of the personal data and the harm that could result if data breaches or leaks were to occur.

Under the new amendments to the Ordinance, where the data user engages a data processor to process personal data on its behalf, the data user must use contractual or other means to:

- prevent unauthorised or accidental access, processing, erasure, or loss of use of the personal data, and
- ensure that the data processor does not retain the personal data for longer than necessary.

BREACH NOTIFICATION

Currently, there is no mandatory legal requirement under the Ordinance for data users to notify authorities or data subjects about data breaches in Hong Kong. The PCPD issued a best practice guide in February 2014 to advocate the development of a privacy management programme and encourage data users to adopt a procedure of notification in handling a data breach. Further guidance was issued in October 2015 on data breach handling and breach notifications.

ENFORCEMENT

The PCPD is responsible for enforcing the Ordinance. If a data user is found to have contravened the data protection principles of the Ordinance, the PCPD may issue an enforcement notice requiring the data user to take steps to rectify the contravention. Failure to abide to the enforcement notice is a criminal offence, punishable by a fine of up to HK$ 50,000 and imprisonment for up to 2 years. In the case of subsequent convictions, additional and more severe penalties apply. Contravention of other requirements of the Ordinance is also an offence. In particular, breach of new provisions relating to direct marketing is punishable by a fine of up to HK$ 1,000,000 and imprisonment of up to 5 years, depending on the nature of the breach.

In addition to criminal sanctions, data subjects aggrieved by contravention of the Ordinance may also seek compensation from the data user through civil action.

ELECTRONIC MARKETING

The new provisions in the Ordinance on direct marketing include, amongst other things, provisions regulating the use and provision of personal data for purposes of direct marketing which may be conducted by any means (electronic or otherwise).

The direct marketing provisions generally require data users who wish to either use or provide personal data for direct marketing purposes to make specific disclosures to the data subjects and obtain consents for such actions. The disclosures include:

- a statement of intention to use/provide their personal data for direct marketing
- a statement that the data user may not use/provide the personal data without the data subjects' consent
- a dedicated channel via which the data subjects may give such consent
- the kind(s) of personal data to be used/provided
- the class(es) of persons to whom the personal data may be provided
- the class(es) of goods/services to be direct marketed, and
- a statement that the personal data may be provided for gain, if applicable.

Furthermore, if the consent was given orally, data users have the additional obligation to send a written confirmation to the data subject confirming the particulars of the consent received. In addition, when data users use personal data for the purposes of direct marketing for the first time, they must inform the subjects that they may opt-out at any time, free of charge.

ONLINE PRIVACY

The principles as stated in the Ordinance also apply in the online environment. For example, under the Ordinance, data users have the obligation to inform data subjects of the purposes for collecting their personal data. If a website uses cookies to collect personal data from its visitors, this should be made known to them. Data users should also inform the visitors whether and how non-acceptance of the cookies will affect the functionality of the website.

KEY CONTACTS

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

HUNGARY

Last modified 27 January 2016

LAW IN HUNGARY

The EU Data Protection Directive 95/46/EC is currently implemented in Hungary by Act No. CXII of 2011 on Informational Self Determination and Freedom of Information which came into force on 1 January 2012 ('Act'). Enforcement is through the National Authority for Data Protection and Freedom of Information ('Authority').

DEFINITIONS

Definition of personal data

Personal data shall mean any data relating to the data subject – in particular name, identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity – and any reference that can be drawn from such data in respect of the data subject. In the course of data processing, such data shall be treated as personal data as long as the connection between the data and the data subject remains restorable. The data shall be considered subject to restoration, if the data controller bears the technical measures necessary for such restoration. Unless the data controller is directly able, by its technical capabilities, to trace the data back to the data subject, data shall not be considered as 'personal data'.

Definition of sensitive personal data

Sensitive personal data shall mean:

- personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade union membership or sex life, and
- personal data concerning health, addictions, or criminal personal data.

NATIONAL DATA PROTECTION AUTHORITY

National Authority for Data Protection and Freedom of Information
Address: H-1125 Budapest, Szilágyi Erzsábet fasor 22/c.

T +36 1 391 1400
F +36 1 391 1410

http:\\www.naih.hu
ügyfélszolgálat@naih.hu

REGISTRATION

If a data controller intends to conduct data processing, it is obliged to file a request with the Authority. Data processing must be registered by the Authority before it can occur. The Authority will charge a fee for registration. The fee that will be charged is currently unknown, but is expected to fall within the range of EUR 20-30.

Should the Authority fail to respond to a request for registration within 8 days of the filing of such a request, data processing may be commenced.

No register is held and thus no request can be filed for processing personal data relating to data subjects' employment, membership, or customer relationship with the data controller. Financial institutions, community service providers and electronic communication service providers are excluded from this exemption, ie they will be obliged to register even if they process the above data.

The notification should include the following information:

- the purpose of processing
- the types of data and the grounds for processing
- the categories of data subjects
- the source
- the categories of data transferred, the recipients and the grounds for transfer
- the name and registered office of the data controller and the data processor, the place where records are stored and/or where processing is carried out, and the data processor's activities in connection with data processing operations
- the name and contact information for the internal data protection officer (if any), and
- the applied technology for data processing.

DATA PROTECTION OFFICERS

The following data controllers and data processors shall appoint or commission an internal data protection officer ('DPO') (holding a law degree, a degree in economics or computer sciences or an equivalent degree in higher education) who is to report directly to the head of the organisation:

- authorities that control or process personal data in respect of nationwide registers, or authorities that control or process employment or criminal records
- financial institutions, and
- telecommunications service providers and public utility companies.

Although the Act does not specify, it is strongly recommended to appoint a Hungarian resident as a DPO, because the various tasks of the DPO require continuous presence and availability of the DPO at the above mentioned organisations.

If a DPO is required, but the data controller or processor fails to appoint one, the Authority may take enforcement actions as detailed below

As a new institution effective from 1 January 2012, the head of the Authority will convene a conference of the DPOs at least once a year to discuss data protection related matters.

COLLECTION & PROCESSING

Personal data may be collected and processed if:

- the data subject has given his or her consent, or
- this is required by an Act or by a decree of the local municipality based on the authorisation conferred by an Act concerning the specific data as defined therein.

Personal data can also be processed if it is impossible to obtain the consent of the data subject or it would cause disproportionate costs and the processing is necessary:

- for compliance with a legal obligation to which the controller is subject, or
- for the purposes of the legitimate interests of a third party, or the controller itself, where the assertion of such interests is proportionate with the interference in data protection rights.

Sensitive data may be processed if:

- the data subject has given his or her explicit consent in writing
- it is necessary to enforce an obligation prescribed by an international treaty, or for the enforcement of a constitutional right set forth in the Fundamental Law of Hungary, or prescribed by an Act for national security or law enforcement purposes regarding personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade union membership or sex life, or
- the data is required by an Act for the purpose of public order in the case of personal data concerning health, addictions, or criminal personal data.

Personal data may be processed only for specified and explicit purposes, where it is necessary for exercising certain rights or fulfilling certain obligations. This purpose must be satisfied in all stages of operations of data processing.

The personal data processed must be essential for the purpose for which it was collected, it must be suitable to achieve that purpose, and it may be processed to the extent and the duration necessary to achieve that purpose.

TRANSFER

Transferring personal data of data subjects within the EEA shall be considered as data transfer within Hungary. Transferring personal data to data processors within the EEA is possible without the consent of the data subjects. Under the Act a data processor is the person that is engaged in the processing of personal data on behalf of the controller, and the data processor is carrying out 'the technical operations in connection with the data management.' In practice an entity will be a data processor for the purposes of the Act where it acts on the basis of the instructions (on behalf) of the data controller and follows the predetermined rules and methodology set by the data controller.

The Act makes it possible to transfer personal data to third countries (ie to countries outside of the EEA) if the conditions (legal bases) of the data processing are satisfied (see above) and an adequate level of protection is afforded in such third countries.*

Adequate level of protection is afforded if: a) this is established by binding legislation of the European Union, or b) there is an international agreement between the third country and Hungary to this effect, or c) using binding corporate rules

within a group of companies. On the basis of the foregoing, the use of EU model clauses may afford adequate protection, however, we note that as a result of the Schrems decision of the Court of Justice of the European Union (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US.

SECURITY

Data controllers, and within their sphere of activity, data processors must ensure personal data protection and must implement technical and organisational measures, as well as adequate procedural rules to enforce the provisions of the Act and other regulations concerning confidentiality and security of data processing.

Personal data must be protected against unauthorised access, alteration, transfer, disclosure, deletion, accidental deletion or damage as well as against being unable to access the data due to the change in the applied technology.

If multiple possibilities for data processing solutions exist, the solution to be chosen should provide a higher level of security for personal data, unless this would result in a disproportionate burden for the data controller.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the Authority or to data subjects.

As an exception, however, electronic communication service providers must immediately report data security breaches to the National Media and Infocommunications Authority under Act No. 100 of 2003 on Electronic Communications.

ENFORCEMENT

Enforcement is through the National Authority for Data Protection and Freedom of Information. The leader of the Authority is the President, nominated by the Prime Minister and appointed by the President of the Republic, for a total term of 9 years.

The Authority has several instruments to enforce compliance, the most important being:

- ordering the correction of inadequate personal data
- ordering the block deletion or termination of illegally controlled personal data
- prohibiting the illegal controlling or processing of personal data
- prohibiting the transfer of personal data to foreign countries
- ordering the notification of the affected party, if the data controller illegally refused to do so, and
- imposing a fine ranging from HUF 100,000 (cca. EUR 350) to HUF 10,000,000 (cca. EUR 35,000)

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be ‘personal data’ for the purposes of the Act).

Also, pursuant to Act 48 of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, unless otherwise provided by specific other legislation, advertisements may be conveyed to natural persons by way of direct contact (hereinafter referred to as ‘direct marketing’), such as through electronic mail or equivalent individual communications only upon the express prior consent of the person to whom the advertisement is addressed. The request for the consent may not contain any advertisement, other than the name and description of the company.

The statement of consent may be made in any way or form, on condition that it contains the name of the person providing it, and – if the advertisement to which the consent pertains may be disseminated only to persons of a specific age – his place and date of birth, furthermore, any other personal data authorised for processing by the person providing the statement, including an indication that it was given freely and in possession of the necessary legal information.

The statement of consent may be withdrawn freely any time, free of charge and without any explanation. In this case all personal data of the person who has provided the statement must be promptly erased from the records and all advertisements must be stopped.

Pursuant to Act 100 of 2003 on Electronic Communications ('EC Act'), applying automated calling system free of any human intervention, or any other automated device for initiating communication in respect of a subscriber for the purposes of direct marketing, providing information, public-opinion polling and market research shall be subject to the prior consent of the subscriber.

ONLINE PRIVACY

The EC Act deals with the collection of location and traffic data by public electronic communications services providers ('CSPs') and use of cookies (and similar technologies).

Traffic Data

With certain special exceptions set out in the EC Act (eg invoicing, collecting subscriber fees, law enforcement, national security and defence), traffic data relating to subscribers and users processed and stored by CSPs while providing such services must be erased or made anonymous when it is no longer needed.

CSPs may use certain traffic data as referred to in the EC Act for the provision of value added services or for marketing purposes subject to the subscriber's or user's prior consent, to the extent necessary for the provision of such services or for marketing purposes. CSPs shall provide the possibility for users or subscribers to withdraw their consent at any time.

Location Data

CSPs shall be authorised to process location data only upon the prior consent of the subscribers or users to whom the data are related, and only to the extent and for the duration as it is necessary for the provision of value added services.

Users and subscribers shall have the right to withdraw their consent at any time.

CSPs shall be required to comply with any request for location information in connection with specific subscribers or users, if made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorisation conferred in specific other legislation, to the extent required to discharge their respective duties.

Cookie Compliance

Pursuant to the EC Act, on the electronic communication terminal equipment of a subscriber or user, information may be stored, or accessed, only upon the user's or subscriber's prior consent granted in possession of clear and comprehensive information, which information *inter alia* includes the purpose of processing.

The competent Hungarian Authorities have not issued any guidance in respect of the interpretation of 'consent' and how this consent should be obtained in practice. General practice is that consent can be obtained via browser settings, however, as mentioned so far this has not been confirmed by the opinion or the guidance of the Authorities yet.

KEY CONTACTS

Zoltán Kozma
Counsel
T +36 1 510 1100
zoltan.kozma@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

ICELAND

Last modified 27 January 2016

LAW IN ICELAND

The governing legislation on data protection is Act No 77/2000 on the Protection and Processing of Personal Data ('Data Protection Act'), which implemented EU Data Protection Directive 95/46/EC.

DEFINITIONS

Definition of personal data

Any data relating to the data subject (identified or identifiable), i.e. information that can be traced directly or indirectly to a specific individual, deceased or living.

Definition of sensitive personal data

Sensitive personal data means data on origin, skin colour, race, political opinions, religious beliefs and other life philosophies; data on whether a man has been suspected of, indicted for, prosecuted for or convicted of a punishable offence; health data, including genetic data and data on use of alcohol, medical drugs and narcotics; data concerning sex life (and sexual behaviour); and data on trade-union membership.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Authority

Raudarárstíg 10
105 Reykjavík

www.personuvernd.is

REGISTRATION

All electronic processing of personal data, which falls under the Data Protection Act, must be notified to the Icelandic Data Protection Authority, by the controller of the data, unless an exemption applies.

For example, there is an exemption for data processing which is necessary and carried out in the regular or standard course of activities, relating solely to those data subjects who have a connection to the activities being performed or the relevant field of work, eg the controller is only processing data related to business associates, customers, employees and members and none of the data processed includes sensitive data.

Notification to the Data Protection Authority is required for any changes to the processing of personal data, which has already been notified.

Notification to the Data Protection Authority must be submitted electronically and in Icelandic.

Certain data processing is also subject to an authorization from the Icelandic Data Protection Authority. For example, processing that involves the collection and disclosure of information related to the financial and credit standing data of individuals must be authorized by the Icelandic Data Protection Authority.

DATA PROTECTION OFFICERS

There is no specific requirement under the Data Protection Act to appoint data protection officers.

Where a controller does not have an establishment in Iceland, but the Data Protection Act is still applicable (e.g., because the controller uses processing equipment in Iceland), the controller must, however, designate a representative established in Iceland. In such cases, the provisions of the Act relating to controllers shall apply to the representative.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject has unambiguously agreed to the processing or given his consent
- the processing is necessary to honour a contract to which the data subject is a party, or to take measures at the request of the data subject before a contract is established
- the processing is necessary to fulfill a legal obligation of the controller
- the processing is necessary to protect vital interests of the data subject
- the processing is necessary for a task that is carried out in the public interest
- the processing is necessary in the exercise of official authority vested in the controller or in a third party to whom data are transferred
- the processing is necessary for the controller, or a third party, or parties to whom data are transferred, to be able to safeguard legitimate interests, except where overridden by fundamental rights and freedom of the data subject, which shall be protected by law.

Where sensitive personal data is processed, one of the above conditions must be met as well as one of a further list of additional conditions. Examples of such additional conditions are if the data subject gives his consent to the processing and/or if the processing is specifically authorized in another Act of law.

The processing must in all events be processed in a fair, appropriate and lawful manner, and the data must be obtained for a specific, explicit and appropriate purpose.

Furthermore, unless an exemption applies, the controller must provide the data subject with notice of certain information, including the identity of the controller, the purpose of the processing, and the recipients of the data.

TRANSFER

The transfer of personal data to a country that does not provide an adequate level of personal data protection is prohibited, unless:

- the data subject has consented to the transfer
- it is necessary for the fulfillment of obligations under international law or as a result of Iceland's membership with an international organization
- such a transfer is authorized in another legislative act

- the delivery is necessary to establish or fulfill a contract between the data subject and the controller
- the transfer is necessary to establish or fulfill a contract in the interest of the data subject
- the delivery is necessary in order to protect the vital interests of the data subject
- the dissemination is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims, or
- the data in question are accessible to the general public.

Countries in the European Economic Area are considered to provide an adequate level of personal data protection, and so are Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, Faroe Islands, Andorra, Israel and Uruguay.

The Icelandic Data Protection Authority can also authorize a transfer of personal data to an insecure third country where a controller adduces adequate (contractual) safeguards with respect to the protection of the rights of the data subject(s).

SECURITY

A controller must implement appropriate technical and organizational measures to protect personal data against unlawful destruction, against accidental loss or alteration and against unauthorized access. The same rule applies to data processors of personal data, in practice, because controllers are required to contractually pass down their security obligations under the Data Protection Act to their processors.

BREACH NOTIFICATION

There is no mandatory requirement in the Data Protection Act to report data security breaches or losses to the Icelandic Data Protection Authority.

ENFORCEMENT

The Icelandic Data Protection Authority is responsible for the enforcement of the Data Protection Act.

Infringements of the provisions of the Data Protection Act, and of regulations issued according to it, are punishable by means of fines or a prison term of up to three years, unless more severe sanctions are provided for in other acts of law. The same punishment shall apply if instructions by the Data Protection Authority are not observed.

If a controller or a processor has processed personal data in violation of the Data Protection Act, rules or instructions by the Data Protection Authority, then the controller may be required to compensate the data subject for the financial damage suffered as a result of the violation.

The Data Protection Authority can furthermore order the cessation of the processing of personal data and the Authority can decide to impose daily fines if its instructions are not complied with, until it concludes that necessary improvements have been made.

ELECTRONIC MARKETING

Based on the Electronic Communications Act No 81/2003 the use of electronic communications systems, including for email and other direct marketing, is only allowed if a subscriber has given prior consent.

If the email address has been obtained in the context of the sale of a good or service, the controller may use it for direct marketing of the controller's own goods or services to customers who have not objected to receiving email marketing from the controller, provided the customers are given the opportunity, free of charge, to object to such use of their email address when it is collected and each time a message is sent.

Further, all marketing emails must include the name and address of the party responsible for the marketing.

ONLINE PRIVACY

There are no provisions in Icelandic legislation that specifically deal with the use of cookies or location data. However, location data and IP addresses are considered personal data under the Data Protection Act.

If the use of cookies leads to the use of IP addresses or other personal data, the processing of such data must comply with the Data Protection Act. The processing is therefore not permissible unless one of the listed conditions is met, in most instances the data subject must consent to the processing of such data.

KEY CONTACTS

LOGOS Legal Services
www.logoslegalservices.com

Hjördís Halldórsdóttir
Partner
T +354 5 400 300
hjordis@logos.is

Áslaug Björgvinsdóttir
Senior Associate
T +354 5 400 300
aslaug@logos.is

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

INDIA

Last modified 27 January 2016

LAW IN INDIA

There is no specific legislation on privacy and data protection in India. However, the Information Technology Act, 2000 (the 'Act') contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically).

India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules). The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal data, including sensitive personal information to comply with certain procedures. It distinguishes both 'personal information' and 'sensitive personal information', as defined below.

In August 2011, India's Ministry of Communications and Information issued a 'Press Note' Technology (Clarification on the Privacy Rules), which provided that any Indian outsourcing service provider/organisation providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is *not* subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

DEFINITIONS

Definition of personal data

The Privacy Rules define the term 'personal information' as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

Definition of sensitive personal data

The Privacy Rules define 'sensitive personal data or information' to include the following information relating to:

- password
- financial information eg bank account/credit or debit card or other payment instrument details
- physical, physiological and mental health condition
- sexual orientation
- medical records and history

- biometric information
- any detail relating to the above clauses as provided to a corporate entity for providing services, and
- any of the information received under the above clauses for storing or processing under lawful contract or otherwise.

Biometrics means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes.

However, any information that is freely available in the public domain is exempt from the above definition.

NATIONAL DATA PROTECTION AUTHORITY

No such authority exists.

REGISTRATION

No requirements.

DATA PROTECTION OFFICERS

Every corporate entity collecting sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests in an expeditious manner but within one month from the date of receipt of grievance.

There is no specific requirement that the data protection officer must be a citizen of or resident of India, nor are they any specific enforcement actions or penalties associated with not appointing a data protection officer correctly. However, appointment of a data protection officer is part of the statutory due diligence process and it is thus imperative that such an officer should be appointed

COLLECTION & PROCESSING

Under the Act, if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

The Privacy Rules state that any corporate entity or any person acting on its behalf, which is collecting sensitive personal information, must obtain written consent (through letter, email or fax) from the providers of that information. However, the August 2011 'Press Note' issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication.

The Privacy Rules also mandate that any corporate entity (or any person, who on behalf of such entity) collects, receives, possess, stores, deals or handles information, shall provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information including sensitive personal information and ensure that the policy is available for view, including on the website of the corporate entity (or the person acting on its behalf). Specifically, the corporate entity must ensure that the person to whom the information relates is notified of the following at the time of collection of sensitive personal information or other personal information:

- the fact that the information is being collected
- the purpose for which the information is being collected

- the intended recipients of the information, and
- the name and address of the agency that is collecting the information and the agency that will retain the information.

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required, and should also ensure that the same is being used for the purpose for which it was collected.

A corporate entity or any person acting on its behalf is obligated to enable the providers of information to review the information they had so provided and also to ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information has to be provided a right to opt out (ie he/she will be able to withdraw his/her consent) even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

TRANSFER

The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or in any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer, if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act.

A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required in the Act.

The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe.

Further, under the Act, it is an offence for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

Thus, contracts should also specifically include provisions:

- entitling the data collector to distinguish between ‘personal information’ and ‘sensitive personal information’ that it wishes to collect/process
- representing that the consent of the person(s) concerned has been obtained for collection and disclosure of personal information or sensitive personal information, and
- outlining the liability of the third party.

SECURITY

A corporate entity possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. The reasonable security practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement ‘reasonable security practices and procedures’ to be adopted by any corporate entity to secure sensitive personal information are procedures that comply

with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the Federal Government. Presently, no such codes of best practices have been approved by the Federal Government.

BREACH NOTIFICATION

The Government of India, has established and authorised the Indian Computer Emergency Response Team (Cert-In), to collect, analyse and disseminate information on cyber incidents, provide forecast and alerts of cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities.

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) impose mandatory notification requirements on service providers, intermediaries, data centres and corporate entities, upon the occurrence of certain 'cyber security incidents'.

Cyber security incidents have been defined to mean any real or suspected adverse events, in relation to cyber security, that violate any explicitly or implicitly applicable security policy, resulting in:

- unauthorised access, denial or disruption of service
- unauhorised use of a computer resource for processing or storage of information
- changes to data, information without authorisation.

The occurrence of the following types of cyber security incidents, trigger the notification requirements under the Cert-In Rules:

- Targeted scanning/ probing of critical networks/ systems
- Compromise of critical information/ system
- Unauthorized access of IT system/ data
- Defacement of websites or intrusion into website & unauthorized changes such as inserting malicious codes, links to external websites
- Malicious code attacks such as spreading virus, worm/ Trojan/ Botnets/ Spyware
- Attacks on servers such as Database, Mail and DNS & Network devises such as Routers
- Identity theft, Spoofing and phishing attacks
- Denial of service (DoS) & Distributed Denial of service (DDoS) attacks
- Attacks on critical infrastructure , SCADA systems and wireless networks
- Attacks on Application such as E-governance and E-commerce etc.

Upon the occurrence of any of the aforementioned events, companies are required to notify the Cert-In within reasonable time, so as to leave scope for appropriate action by the authorities. However, it is important to follow 'breach notice obligations', which would depend upon the "*place of occurrence of such breaches",* and whether or not Indian customers have been targeted. The format and procedure for reporting of cyber security incidents have been provided by Cert-In on its official website.

ENFORCEMENT

Civil penalties of up to EUR 694,450 for failure to protect data including sensitive personal information may be imposed by an Adjudicating Officer; damages in a civil suit may exceed this amount.

Criminal penalties of up to 3 years imprisonment or a fine up to EUR 6,950, or both for unlawful disclosure of

information.

ELECTRONIC MARKETING

The Act does not refer to electronic marketing directly. However, dishonestly receiving date, computer database or software is an offence.

The Privacy Rules also provide the right to "opt out" of email marketing, and the company's privacy policy must address marketing and information collection practices. Further, Do Not Call (DNC) Registry is effectively implemented by the Telecom Regulatory Authority of India (TRAI). Tele-marketing companies may lose their license for repeated violation of DNC norms.

ONLINE PRIVACY

There is no regulation of cookies, behavioural advertising or location data. However, it is advisable that user consent is obtained by inserting appropriate disclaimers.

However, the IT Act contains both civil and a criminal offences for a variety of computer crimes:

- any person who introduces or causes to be introduced any computer contaminant into any computer, computer system or computer network may be fined up to EUR 694,450 (by an Adjudicating Officer); damages in a civil suit may exceed this amount. Under the IT Act, 'computer contaminant' is defined as any set of computer instructions that are designed:
    - to modify, destroy, record, or transmit data or programmes residing within a computer, computer system or computer network, or
    - by any means to usurp the normal operation of the computer, computer system or computer network, and
- any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, is subject to a prison term of up to 3 years and fine up to EUR 1,390.

KEY CONTACTS

Vakul Corporate Advisory Pvt. Ltd

Vakul Sharma
Managing Partner
T +91 11 47025460
vakul@vakulcorp.com

Seema Sharma
Senior Partner
T +91 11 47025460
seema@vakulcorp.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

INDONESIA

Last modified 27 January 2016

LAW IN INDONESIA

Specific Regulations

In Indonesia, as of the date of this publication there is no general law on data protection. However, there are certain regulations concerning the use of electronic data. The primary sources of the management of electronic information and transactions are Law No. 11 of 2008 regarding Electronic Information and Trasactions ("**EIT Law**") and its main implementing regulation, Government Regulation No. 82 of 2012 regarding Provisions of Electronic systems and Transactions ("**Reg. 82**").

However, a new draft Bill on the Protection of Private Personal Data (the "**Bill**") is currently being discussed and there is reason to believe that this Bill may come into law in 2016, although the exact date remains uncertain and the Bill is still to be considered by the House of Representatives. If passed, this will become Indonesia's first comprehensive law to specifically deal with the issue of data privacy.

In addition to the provisions under EIT Law and Reg. 82, there are also a series of regulations which also cover certain provisions which may relate to data protection, such as:

Telecommunications Sector

Article 40 of Law No. 36 of 1999 regarding Telecommunications ('Telecommunications Law') provides that any person is prohibited from any kinds of tapping on information transmitted through any kinds of telecommunications network. Furthermore, Article 42 of the Telecommunications Law stipulates that any telecommunications services operator has to keep confidential any information transmitted and/or received by telecommunications service subscriber through telecommunications networks and/or telecommunications services provided by the relevant operator.

Public Information Sector

Article 6 of Law No. 14 of 2008 regarding Disclosure of Public Information provides that information relating to personal rights may not be disclosed by public bodies. Furthermore, Article 17 of the relevant law, together with other laws,prohibits the disclosure of private information of any person, particularly that which concerns family history; medical and psychological history; financial information (including assets, earnings and bank records)and evaluation records concerning a person's capability/recommendation/intellectual, formal/ informal education records.

.

Banking and Capital Markets Sectors

Data privacy in this sector is regulated under Law 7 of 1992 as amended by Law 10 of 1998 on Banking ('Banking Law') and Law 8 of 1995 on Capital Markets ('Capital Markets Law') respectively. The regulations apply to both individuals and corporate data.

Bank Indonesia's Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilisation of Information Technology by the Bank stipulates that the bank's customer data transfer (by way of establishing a data centre or a data processing outside Indonesia territory) necessitates prior approval being obtained from Bank Indonesia.

DEFINITIONS

Definition of personal data

Reg. 82 defines personal data as: data of an individual, which is stored, maintained and which correctness is preserved and of which its confidentiality is protected (including under the EIT Law and Reg 82).

Definition of sensitive personal data

Currently, there is no specific definition on sensitive personal data under the prevailing laws and regulations.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority for data privacy in general in Indonesia.

For example, the Indonesian Financial Services Authority ('FSA') has the authority to act as the regulator of data privacy in the capital markets sector (since 31 December 2012) and with regard to banks' customer data privacy issues (since 31 December 2013).

However, please note that article 65 of Reg. 82 provides that a business enactor who operates electronic transactions may be certified by a Competence Certification Body (*Lembaga Sertifikasi Keandalan*) which may be a domestic Indonesian (but currently no such domestic bodies exist) or foreign competence certification body.

REGISTRATION

Indonesia does not maintain a register of controllers or of processing activities.

DATA PROTECTION OFFICERS

There is no requirement in Indonesia for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Both EIT Law and Reg. 82 specifically regulate the obligation to obtain "consent" from the owner of the personal data in the case of data collection, use and processing.

Reg. 82 provide the specific provisions on the obligation for Electronic System Providers to public services to set up a data centre and disaster recovery centrein Indonesia, namely:

- before an Electronic System for public services is implemented, the provider of an Electronic System must register with the Minister of Communication and Information and Technology ("MOCI")
- in providing the provision of an Electronic System, the provider should ensure secrecy, totality and the availability of the Personal Data it manages. The provider should also ensure that the obtaining, the consumption, and usage of Personal Data is based on the consent of the Personal Data owner, except if

regulated otherwise[1]. Further the provider should ensure that the usage or dislosure of data is done based on the consent of Personal Data and is in line with the objectives as disclosed to the relevant owner at the time of obtaining the data[2] and

- the provider of the Electronic System is also obliged to provide audit track records of the Electronic System.

[1] Article 15 (1) (b) of Reg. 82.

[2] Article 15 (1) (c) of Reg. 82.

TRANSFER

Reg. 82 regulates the transfer of data in Article 22 paragraph 2 which provides in any case that in the implementation of an Electronic System and/or Electronic Document aimed to transfer Electronic Information and/or Electronic Document, the Electronic Information and/or Electronic Document must be unique and (the provider shall) explain the control and posession of the Electronic Information and/or Electronic Document.

Neither the EIT Law nor Reg. 82 specifically restricts or permits the transfer of data, including personal data, out of Indonesia (the regulations are silent on this issue). Existing restrictions are not related to locationor movement of the data (including out of Indonesia), butare related to whether the data, particularly personal data, is obtained and used inaccordance with the purpose conveyed to the data owner at the time the data was acquired)[1].

[1] See Article 15 (1) (b) and (c) of Reg. 82

SECURITY

The obligations of Electronic System Providers are regulated under Reg. 82 and amongst other things shall amongst other things:

- guarantee the confidentiality of the source code of the software
- ensure agreements on minimum service level and information security towards the information technology services being used as well as security and facility of internal communication security it implement
- protect and ensure the privacy and personal data protection of users
- ensure the appropriate lawful use and disclosure of the personal data
- provide data centre and disaster recovery centre (for Electronic System Providers for public services)
- provide the audit records on all Provision of Electronic Systems activities, and
- provide information in the Electronic System based on legitimate request from investigators for certain crimes.

In the telecommunication sector, Article 19 of Minister of Communication and Informatics Regulation No. 26/PER/M.KOMINFO/05/2007 regarding the Security and Utilisation of Internet Protocolbased Telecommunications Network (as amended) ("MR 26/2007") also provides that the telecommunication service provider is responsible for data storage due to its obligation to record its log file for at least three months.

BREACH NOTIFICATION

Article 15 Paragraph 2 of Reg. 82 provides that the provider of an Electronic System must provide written notification to the owner of personal data, upon its failure to protect the personal data.

Article 20 Paragraph 3 of Reg. 82 provides that the provider of an Electronic System must make the utmost effort to protect personal data and to immediately report any failure/serious system interference/disturbance to a law enforcement official or the Supervising and Regulatory Authority of the relevant sector.

ENFORCEMENT

In Indonesia, the sanctions for breaches of data privacy are found under the relevant legislation and are essentially fines. Imprisonment may be imposed in severe instances such as in the event of intentional infringement.

- the EIT Law provides criminal penalties ranging from; Rp. 600,000,000 fine to Rp. 800,000,000 and/or 6 to 8 years imprisonment for unlawful access; Rp. 800,000,000 fine and/ or 10 years imprisonment for interception/wiretapping of transmission; Rp. 2,000,000,000 to Rp. 5,000,000,000 and/or 8 to 10 years imprisonment for alteration, addition, reduction, transmission, tampering, deletion, moving, hiding Electronic Information and/or Electronic Records.
- Failure to comply with Reg. 82 is subject to administrative sanctions (which do not eliminate any civil and criminal liability). These administration sanctions are in the forms of:
    - written warning
    - administrative fines
    - temporary dismissal, or
    - expelled from the list of registrations (as required under the regulation)

Banking Law

Under Article 47 of the Banking Law, any commissioner, director or employee of a bank or its affiliates who intentionally provides information which has to be kept secret may be sentenced to imprisonment for not less than two years but not more than four years, and fined at least four billion but not more than eight billion Indonesian Rupiah.

Capital Markets Law

Under Capital Markets Law, the Financial Services Authority (Previously BAPEPAM LK) is empowered to impose the following administrative sanctions for breaches of the provisions dealing with data protection). The sanctions comprise:

- a written reminder
- a fine
- limitations on business
- suspension of business
- revocation of business licence
- cancellation of approval, and
- cancellation of registration

ELECTRONIC MARKETING

EIT Law and Reg. 82 do not specifically address electronic marketing.

Article 25 of the EIT Law provides that an Internet website, amongst other things, is acknowledged and protected as an Intellectual Property (IP) and consequently, should fall under the ambit of the relevant IP laws, which may in certain cases fall under the Indonesian Copyright Law.

ONLINE PRIVACY

There are currently no laws and regulations concerning cookies and location data.

However, if the data collected by cookies or location data is obtained by the unlawful access of another party's electronic information, this is subject to 6 to 8 years imprisonment and/or a fine of Rp. 600,000,000 to Rp. 800,000,000.

KEY CONTACTS

Ivan Almaida Baely & Firmansyah
www.iab-net.com

Erwin Purba
Special Counsel
T +62 21 5790 5090
erwin.purba@iab-net.com

Aston Goad
Foreign Legal Consultant
T +62 21 5790 5090
aston.goad@iab-net.com

Tania Faramutia
Associate
T +62 21 5790 5090
tania.faramutia@iab-net.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

IRELAND

Last modified 21 January 2016

LAW IN IRELAND

The core Irish data protection law is comprised in the Data Protection Act 1988 ('1988 Act') as amended by the Data Protection (Amendment) Act 2003 ('2003 Act') (together the Data Protection Acts ("DPA")). The 2003 Act implemented the EU Data Protection Directive (95/46/EC) ("Data Protection Directive"). In addition to the DPA, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ('ePrivacy Regulations') set out data protection rules in relation to direct marketing and electronic networks and services, including location data and cookies.

DEFINITIONS

Definition of personal data

Personal data is defined as data relating to a living individual who is or can be identified from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller.

Definition of sensitive personal data

Sensitive personal data means personal data as to:

- the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject
- whether the data subject is a member of a trade union
- the physical or mental health or condition or sexual life of the data subject
- the commission or alleged commission of any offence by the data subject, or
- any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Data Protection Commissioner ('DPC')

Canal House Station Road Portarlington Co. Laois
Ireland

LoCall 1890 25 22 31

T +353 57 868 4800
F +353 57 868 4757

info@dataprotection.ie
www.dataprotection.ie

REGISTRATION

All data controllers and data processors are required to register with the DPC unless exempt.

The Irish registration regime contains wide exemptions for certain categories of processing that do not trigger a registration obligation. There are also certain categories of data controller and data processor that are subject to an absolute obligation to register.

The DPA exempts:

- not for profit organisations, provided they only process personal data relating to their activities
- data controllers and data processors who process personal data kept in a public register, and
- data controllers and data processors who only process manual data.

The Data Protection Act 1988 (Section 16(1)) Regulations 2007 ('2007 Regulations') also exempt from registration:

- data controllers that only process employees' human resources data in the normal course of personnel administration
- candidates for political office and elected representatives
- schools, colleges, universities and similar educational institutions
- solicitors and barristers
- data controllers who process customer and supplier data in the context of normal commercial activity
- companies who process personal data of past and present shareholders, directors or other officers in complying with the Irish Companies Acts
- data controllers who process personal data for the purpose of publishing journalistic, literary or artistic material, and
- data controllers or data processors who operate under a statutory data protection code of practice.

Data processors that process personal data on behalf of any of the above categories of data controller are also not required to register.

The 2007 Regulations impose an absolute obligation to register on banks, insurance undertakings, direct marketing firms, debt collection agencies, credit reference agencies, health professionals, anyone processing genetic data, ISPs and telecoms companies. Any data processor that processes personal data on behalf of a data controller that falls into one of these categories is also obliged to register. A failure by a data controller or processor to register, when required to do so, is an offence punishable by fines up to EUR€100,000.

Data controllers and/or data processors are obliged to renew their registration annually. The DPC may refuse an application for registration under certain conditions. There is a right of appeal against a refusal to the Circuit Court.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a data protection officer but it would be best practice to do so. The DPC recommends that data controllers appoint a co-ordinator to deal with subject access requests. Where a data protection officer is appointed, this information should be supplied to the data subjects.

COLLECTION & PROCESSING

The DPA transposes the data protection principles from the Data Protection Directive, which need to be complied with in relation to the collection and processing of personal data.

In addition to complying with the data protection principles, all processing of personal data must comply with one of a number of legitimate processing conditions contained in the DPA.

These include that:

- the data subject has given his or her consent to such processing
- the processing is required for the performance of a contract to which the data subject is a party
- the processing is necessary for compliance with a legal obligation to which the data controller is subject
- the processing is to prevent an injury or other damage to the health of the data subject
- the processing is to protect an individual's vital interests
- the processing is for the administration of justice, or
- the processing is for the purposes of the legitimate interests pursued by a data controller.

If sensitive personal data is being processed, then an additional set of processing conditions need to be satisfied. These include the 'explicit' consent of the data subject. The grounds for processing sensitive data are quite restrictive and it can sometimes be difficult to legitimise the processing of sensitive personal data.

TRANSFER

The DPA contains a number of restrictions on the transfer of personal data by a data controller to a country or territory outside of the European Economic Area ('EEA'). Under the DPA, such transfers may not take place unless the receiving country ensures an adequate level of protection for the privacy of data subjects in relation to the processing of their personal data. A limited number of countries are recognised by the European Commission as having this level of protection.

Otherwise under the DPA, it is only possible to transfer personal data outside the EEA if:

- the data subject has consented to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the data controller
- the transfer is necessary for the performance of a contract between the data controller and someone other than the data subject, and the contract is entered into at the request of the data subject, or the contract is in the interests of the data subject
- the transfer is necessary for reasons of public interest
- the transfer is necessary under some international obligation of the State

- the transfer is required or authorised by law
- the transfer is necessary for obtaining legal advice
- the transfer is necessary in order to prevent personal injury or damage to the health of the data subject, or
- the transfer is done under one of the EU Approved Model Clauses.
- the transfer is necessary to protect the data subject's vital interests
- the personal data to be transferred are an extract from a statutory public register
- the transfer is subject to standard contractual clauses approved by the EU Commission
- the transfer of data is subject to binding corporate rules ("BCRs").

The DPC recognises the use of BCRs, and the Irish DPC has agreed to abide by the mutual recognition procedure. Multinational companies must draft and submit draft BCRs to the DPC for its approval. The Irish DPC acted as the lead authority for approval of the Intel Corporation's BCRs in January 2012.

Formerly, transfers of data from the EEA to the US could take place (in the absence of fulfilling one of the exceptions above) where the recipient in the US had signed up to the Safe Harbor regime. This is no longer the case since the Court of Justice of the European Union held in *Schrems v. Data Protection Commissioner* (C-362/14) that the European Commission Decision underlying Safe Harbor (Decision 2000/520/EC) is invalid.

SECURITY

Data controllers and data processors must take appropriate security measures against unauthorised access to or unauthorised alteration, disclosure or destruction of, personal data, particularly where the processing involves the transmission of data over a network and against all other forms of processing.

As to the level of security required, data controllers and data processors must put in place appropriate security provisions for the protection of personal data, having regard to:

- the current state of technological development
- the cost of implementing security measures
- the nature of the personal data, and
- the harm that might result from unauthorised processing or loss of the data concerned.

Data controllers and data processors are also obliged to take all reasonable steps to ensure that their employees and other persons at the place of work concerned are aware of and comply with the relevant security measures.

These requirements extend to both technical and organisational security measures. Data controllers should have appropriate access controls in place, and be able to monitor the access to their systems and records. Access should be limited according to sensitivity and on a "need to know" basis.

BREACH NOTIFICATION

The DPC has published a Personal Data Security Breach Code of Practice('Code') which states that the DPC must be notified of any situation where personal data has been put at risk of unauthorised disclosure, loss, destruction or

alteration. There is a limited exception to this requirement where the disclosure:

- affects less than one hundred individuals
- the loss of sensitive personal or financial data is not involved, and
- the affected individuals have been informed.

Under the ePrivacy Regulations, data breaches in relation to electronic communication networks or services must be notified to the Data Protection Commissioner. Where the breach is likely to affect the personal data or privacy of a subscriber, affected subscribers must also be notified.

In very limited circumstances, data controllers can take the view that affected data subjects do not need to be notified if measures have been taken which will make the data inaccessible or unintelligible to unauthorised users; such technical measures could include encryption.

ENFORCEMENT

The DPC is responsible for the enforcement of the DPA and the ePrivacy Regulations.

The DPC must investigate any complaints which he receives from individuals who feel that personal information about them is not being treated in accordance with the DPA, unless she is of the opinion that such complaints are "frivolous or vexatious". The DPC can also launch investigations on her own initiative, where she is of the opinion that there might be a breach of the DPA, or where she considers it appropriate in order to ensure compliance with the DPA. Authorised officials of the DPC have legislative powers of entry, inspection and interrogation to support these investigations. The DPC carried out 38 audits and inspections in 2014, prioritising multinational technology companies and major public-sector organisations.

A breach of specific provisions of the DPA can result in criminal liability. These include:

- the failure of a data controller or data processor to register with the DPC
- the disclosure of personal data which was obtained without authority
- the failure to comply with a DPA enforcement notice
- failure to comply with a DPC prohibition notice on transfer of personal data outside the State
- failure to comply with a DPC notice requiring information, or knowingly providing false or misleading information in response to such a notice
- knowingly supplying false or misleading information as part of a registration with the DPC, and
- failure to comply with an authorised officer of the DPC.

Persons found guilty of offences under the DPA may be liable:

- on summary conviction (before a district judge sitting alone), to a fine not exceeding EUR 4,000, or
- on conviction on indictment (before a judge and jury), to a fine not exceeding EUR 100,000.

It should also be noted that under the DPA personal criminal responsibility may be attached to a director or officer of a company which is found guilty of an offence “committed with the consent or connivance” of that director or officer.

Breaching other provisions of the DPA do not in themselves give rise to criminal liability, but the DPC may investigate the incident and issue an ‘Enforcement Notice’ compelling a data controller to comply with the DPA. Failure to comply with an Enforcement Notice is an offence.

The ePrivacy Regulations prescribe fines for failure to report data breaches, inadequate security measures and sending of unsolicited communications (spam) with regard to electronic communication networks and services.

In addition to specific penalties arising out of enforcement actions, a breach of the DPA can also give rise to reputational damage, particularly if the DPC publishes details of the breach in his Annual Report or issues a press release (as he

does from time to time).

In 2014 the DPC investigated 960 complaints. The majority of these complaints (521 or 54.3%) related to subject access requests. In addition, 176 complaints (or 18.3%) related to violations of the ePrivacy Regulations.

As a result of the ruling of the CJEU in *Google Spain v AEPD and Mario Costeja* (Case C-131/12) (commonly known as the "Google" Spain ruling), a new category of complaint - Internet Search Result Delisting - emerged in 2014. This ruling confirmed that users may request search engines, under certain conditions, to remove the links to information affecting their privacy specifically where a search has been conducted on the name of that individual. The DPC received 32 such complaints against search engines.

ELECTRONIC MARKETING

The ePrivacy Regulations implement the anti-spam rules set out in Article 13 of the Privacy and Electronic Communications Directive 2002/58/EC (as amended by the Citizens' Rights Directive). These regulations came into effect on 1 July 2011. Electronic mail includes text messages (SMS), voice messages, sound messages, image messages, multimedia message (MMS) and email messages.

Direct marketing emails can generally only be sent to users with their prior consent. A limited exemption is available for direct marketing emails sent to existing customers promoting other products or services similar to those previously purchased by that consumer (such emails can only be sent for 12 months, the customer must have been given the opportunity to object when the details were collected and the product or service being marketed must be a product or service offered by the person with the existing relationship with the customer). B2B direct marketing emails can generally be sent unless the recipient has informed the sender that it does not consent to the receipt of such messages.

The identity of the sender must not be disguised or concealed and the recipient must be offered an opt-out.

Direct marketing calls (excluding automated calls) may be made to a landline provided the subscriber has not previously objected to receiving such calls or noted his or her preference not to receive direct marketing calls in the National Directory Database. Direct marketing calls cannot be made to a mobile phone without prior consent.

One cannot send a direct marketing fax to an individual subscriber in the absence of prior consent. One can send such a fax to a corporate subscriber unless that subscriber has previously instructed the sender that it does not wish to receive such communications or has recorded a general opt-out to receiving such direct marketing faxes in the National Directory Database.

Breach of these anti-spam rules is a criminal offence. On a summary prosecution (before a judge sitting alone) a maximum fine of EUR 5,000 per message sent can be handed down. On conviction on indictment (before a judge and jury) a company may be fined up to EUR 250,000 per message sent and an individual may be fined up to EUR 50,000 per message.

ONLINE PRIVACY

Cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The 2011 Regulations expressly refer to the use of browser settings as a means to obtain consent. There is no express requirement for consent to be 'prior' to the use of a cookie. A user must be provided with 'clear and comprehensive information' about the cookie (including, in particular, its purposes). This information must be prominently displayed and easily accessible. The methods adopted for giving information and obtaining consent should be as 'user friendly' as possible.

The DPC has provided regulatory guidance on the use of cookies which can be accessed at: http://www.dataprotection.ie/documents/guidance/Electronic_Communications_Guidance.pdf.

Location Data

One cannot process location data unless either:

- such data has been made anonymous, or
- user consent has been obtained.

A provider of electronic communication networks or services or associated facilities (ie a telco) must inform its users of:

- the type of location data (other than traffic data) that will be processed
- the purpose and duration of the processing, and
- whether the data will be transmitted to a third party to provide a value added service. Users can withdraw their consent to the processing of location data.

KEY CONTACTS

Mason Hayes & Curran
www.mhc.ie/

Philip Nolan
Partner and Head of Commercial Department
T +353 1 6145078
pnolan@mhc.ie

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

ISRAEL

Last modified 27 January 2016

LAW IN ISRAEL

The laws that govern the right to privacy in Israel are the Basic Law: Human Dignity and Liberty, 5752 - 1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the 'PPL') and the guidelines of ILITA (as defined below).

DEFINITIONS

Definition of Personal Data

Personal Data, as defined under the PPL, means: data regarding the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

Definition of Sensitive Personal Data

Sensitive Data, as defined under the PPL, means: data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; and other information if designated as such by the Minister of Justice with the approval of the Constitution, Law and Justice Committee of the Knesset. No such determination has been made to date.

NATIONAL DATA PROTECTION AUTHORITY

The Israeli Law, Information and Technology Authority ("ILITA"), established in September 2006, as determined by Israel's Government decision no. 4660, dated 19.01.2006.

REGISTRATION

Subject to certain exceptions, database registration is required to the extent one of the following conditions are met:

- the database contains information in respect of more than 10,000 data subjects
- the database contains sensitive information
- the database includes information on persons, and the information was not provided by them, on their behalf or with their consent
- the database belongs to a public entity, or
- the database is used for direct-marketing services.

A database is defined under the PPL as a collection of data, stored by magnetic or optic means and intended for computer processing, consequently excluding non-computerized collections.

In 2005, the Ministry of Justice set up a committee generally known as the 'Schoffman Committee' which recommended relaxing registration of ‘ordinary’ databases and focusing on specific categories of information (eg medical data, criminal

records or information about a person's political or religious beliefs). However, to date, the Schoffman Committee recommendations have not crystallized into binding legislation.

DATA PROTECTION OFFICERS

Appointment of a Data Protection Officer is required by an entity meeting one of the following conditions:

- a possessor of five databases that require registration
- a public body as defined in section 23 to the POPL, or
- a bank, an insurance company or a company engaging in rating or evaluating credit.

Failure to nominate a Data Protection Officer when required to do so may result in criminal sanctions, including administrative fines. The PPL does not require that the Data Protection Officer should be an Israeli citizen or resident.

COLLECTION & PROCESSING

The collection, processing or use of personal data is permitted subject to obtaining the informed consent of the data subjects. Such consent should adhere to purpose, proportionality and transparency limitations. As such, consent should be obtained for specific purposes of use, the processing and use of personal data should be proportionate to those purposes, and data subjects should have the right to inspect and correct their personal information. The data subject's consent must be re-obtained for any change in the purpose of use.

Any request for consent from a data subject to have his or her personal data stored and used within a database must be accompanied by a notice indicating:

- whether there is a legal requirement to provide the information
- the purpose for which the information is requested
- the recipients of the data, and
- the purpose(s) of use of the data.

Retaining outsourcing services for the processing of personally identifiable information is subject to the ILITA's Guidelines on the Use of Outsourcing Services of Processing Personal Information (Guideline 2 2011) dated 10 June 2012 ('Outsourcing Guidelines'). The Outsourcing Guidelines include, *inter alia*, factors to be taken into consideration when deciding to use outsourcing services, specific provisions to be included within the data transfer agreement and data security requirements. Processing of personally identifiable information in certain sectors is subject to additional outsourcing requirements.

Entities subject to separate outsourcing guidelines are for example entities supervised by the Commissioner of the Capital Market, Insurance and Savings and entities supervised by the Banking Supervision Department of the Bank of Israel. On 10 September 2014, the Banking Supervision Department of the Bank of Israel issued draft guidelines regarding risk management in cloud computing services used by Israeli banking corporations. Among other various restrictions, the draft guidelines set forth an obligation on supervised entities to receive the approval of the Supervisor of Banks prior to using cloud computing services.

TRANSFER

The transfer of personal data abroad is subject to the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 57612001, pursuant to which personal data may be transferred abroad only to the extent that:

- the laws of the country to which the data is transferred ensure a level of protection, no lesser than the level of protection of data provided for by Israeli Law; or
- one of the following conditions is met:
    - the data subject has consented to the transfer;

- the consent of the data subject cannot be obtained and the transfer is vital to the protection of his or her health or physical wellbeing;
- the data is transferred to a corporation under the control of the owner of the database from which the data is transferred, provided that such corporation has guaranteed the protection of privacy after the transfer;
- the data is transferred to an entity bound by an agreement with the database owner, to comply with the conditions governing the use of the data as applicable under Israeli Laws, mutatis mutandis;
- data was made available to the public or was opened for public inspection by legal authority;
- transfer of data is vital to public safety or security;
- the transfer of data is required by Israeli Law; or
- data is transferred to a database in a country:
    - which is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data; or
    - which receives data from Member States of the European Community, under the same terms of acceptance*, or
    - in relation to which the Registrar of Databases announced, in an announcement published in the Official Gazette (Reshumot), that it has an authority for the protection of privacy, after reaching an arrangement for cooperation with that authority.

      * Following the decision of the ECJ in Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, ILITA issued a statement on October 15, 2015, according to which US safe harbour certified entities would not fall under the foregoing condition, without derogating from all other conditions.

When transferring personal data abroad, the database owner is required to enter into a data transfer agreement with the data recipient, pursuant to which the recipient undertakes to apply adequate measures to ensure the privacy of the data subjects and guarantees that the data shall not be further transferred to any third party.

The foregoing data transfer agreement must also comply with additional restrictions, to the extent that the recipient provides outsourcing services, as set forth in the Outsourcing Guidelines.

On January 31, 2011, the European Commission, on the basis of Article 25(6) of directive 95/46/EC, determined that the State of Israel ensures an adequate level of protection with regard to automated processing of personal data.

SECURITY

The owner, possessor, manager and Data Protection Officer (if applicable) of a database, are each responsible for the data security of the database. ILITA has circulated to the public a draft bill for Protection of Privacy Regulations (Information Security in Databases) 2010 (updated version dated June 3, 2012) imposing detailed data security obligations in respect of databases ('Draft Regulations'). Currently, these are considered best practices; however, if the regulations are passed they will become law

BREACH NOTIFICATION

Currently there is no Israeli statute which requires breach notification. However, ILITA's Outsourcing Guidelines refer to the Draft Regulations as a model for drafting a security protocol to be applied on data processing outsourcing

agreements. Pursuant to the Draft Regulations, notice of security breaches of databases should be made to both to the database owner and to ILITA.

ENFORCEMENT

ILITA has the authority and obligation to supervise compliance and enforce the provisions of the PPL and appoint inspectors to carry out those activities.

Breach of the PPL may result in both civil and criminal sanctions, including administrative fines, 1-5 years of imprisonment, and the right to receive statutory damages under civil proceedings without the need to prove actual damages.

The current draft bill for the 12th Amendment of the PPL provides ILITA with the ability to conduct criminal investigations and to impose monetary sanctions in the amount of up to NIS 3.2 million. The draft bill has passed its first reading, but has yet to pass the approval of the Knesset Constitution, Law and Justice Committee; thereafter it would need to also pass the second and third readings, in order to become a binding piece of legislation.

ELECTRONIC MARKETING

Unsolicited marketing is regulated under the Communications Law (Telecommunications and Broadcasting), 1982 (the 'Anti Spam Act'). The Anti Spam Act prohibits, subject to certain exceptions, advertising by means of automated dialing, fax or text messages without first obtaining the recipient's initial opt-in prior consent; all such communications also must contain an opt-out/ unsubscribe option.

Furthermore, the PPL governs the possession and management of databases intended for direct mailing service and imposes restrictions in connection therewith, including a database registration requirement specifying the purpose of direct mailing and specific record-keeping requirements.

ONLINE PRIVACY

The PPL does not specifically address online privacy, cookies and/or location data, all of which are governed by the general restrictions detailed above, including the requirements imposed on processing databases and direct marketing and the consent, purpose and proportionality restrictions.

The PPL governs information "about a person", as such depending upon the circumstances at hand, any non-identifiable and anonymous information (which cannot be re-identified) may reasonably be interpreted as falling outside the confines of the PPL limitations.

KEY CONTACTS

Goldfarb Seligman & Co., Law Offices
www.goldfarb.com

Sharon Aloni
Partner
T +972 (3) 608 9834
sharon.aloni@goldfarb.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

ITALY

Last modified 12 January 2016

LAW IN ITALY

The Italian law applicable on privacy issues is the Legislative Decree no. 196 of 30 June 2003 (C*odice in materia di protezione dei dati personali*, the 'Privacy Code'). The Privacy Code implements Directives 95/46/EC, 2002/58/EC and 2009/12/EC.

DEFINITIONS

Definition of personal data

Pursuant to section 4 of the Privacy Code, 'personal data' shall mean any information relating to individuals who are or can be identified, even indirectly, by reference to any other information including a personal identification number.

Definition of sensitive personal data

Pursuant to Section 4 of the Privacy Code, 'sensitive data' shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade unionist character, as well as personal data disclosing health and sex life.

NATIONAL DATA PROTECTION AUTHORITY

Garante per la protezione dei dati personali

Piazza di Monte Citorio n. 121 - 00186 *ROMA*

T +39 06.696771
F +39 06.69677.3785

www.garanteprivacy.it, the 'Garante'

REGISTRATION

Pursuant to Section 37 of the Privacy Code, a data controller shall notify the processing of personal data he/she intends to perform exclusively if said processing concerns:

- genetic data, biometric data, or other data disclosing geographic location of individuals or objects by means of an electronic communications network
- data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of

health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure

- data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade-union character
- data processed with the help of electronic means aimed at profiling the data subject and/ or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users
- sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample based surveys, and
- data stored in ad hoc databases managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

DATA PROTECTION OFFICERS

There is no legal requirement in Italy for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

As a general rule, processing of personal (non sensitive) data by private entities or profit seeking public bodies is only allowed if the data subject gives his/her express consent (Section 23 of the Privacy Code).

The data subject's consent is deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with a privacy information notice compliant with Section 13 of the Privacy Code.

Nevertheless, pursuant to Section 24 of the Privacy Code, consent is not required if the processing of personal (non sensitive) data:

- is necessary to comply with an obligation imposed by a law, regulations or EU legislation
- is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract
- concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations and modalities laid down by laws, regulations and EU legislation with regard to their disclosure and publicity
- concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy
- is necessary to safeguard life or bodily integrity of a third party. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted
- is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefore by complying with the legislation in force concerning business and

industrial secrecy, dissemination of the data being ruled out

- is necessary to pursue a legitimate interest of either the data controller or a third party recipient in the cases specified by the *Garante* on the basis of the principles set out under the law, unless said interest is overridden by the data subject's rights and fundamental freedoms, dignity or legitimate interests, dissemination of the data being ruled out

- except for external communication and dissemination, is carried out by non profit associations, bodies or organisations, recognised or not, with regard either to entities having regular contacts with them or to members in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with the information notice provided for by Section 13 of the Privacy Code

- is necessary exclusively for scientific and statistical purposes in compliance with the respective codes of professional practice referred to in Annex A) of the Privacy Code, or else exclusively for historical purposes in connection either with private archives that have been declared to be of considerable historical interest pursuant to Section 6(2) of legislative decree no. 499 of 29 October 1999, adopting the consolidated statute on cultural and environmental heritage, or with other private archives pursuant to the provisions made in the relevant codes

- concerns information contained in the CVs as per Section 13(5 bis) of the Privacy Code, or

- except for dissemination and subject to Section 130 the Privacy Code, concerns communication of data between companies, bodies and/or associations and parent, subsidiary and/or related companies pursuant to Section 2359 of the Civil Code, or between the former and jointly controlled companies, or between consortiums, corporate networks and/or corporate joint ventures and the respective members, for the administrative and accounting purposes specified in Section 34(1 ter) of the Privacy Code, providing such purposes are expressly referred to in a decision that shall be disclosed to data subjects jointly with the information notice referred to in Section 13 of the Privacy Code

Sensitive data may only be processed with the data subject's written consent and the *Garante's* prior authorisation, by complying with the prerequisites and limitations set out in the Code as well as in laws and regulations, unless:

- the data concerns members of religious denominations and entities having regular contact with said denominations for exclusively religious purposes, on condition that the data are processed by the relevant organisations or bodies recognised under civil law and are not communicated or disseminated outside said denominations. The latter shall lay down suitable safeguards with regard to the processing operations performed by complying with the relevant principles as set out in an authorisation by the *Garante*

- the data concerns affiliation of trade unions and/or trade associations or organisations to other trade unions and/or trade associations, organisations or confederations, or

- the data contained in CVs under the terms set forth in Section 13(5 bis) of the Privacy Code.

Sensitive data may also be processed without consent, subject to the *Garante's* authorisation:

- if the processing is carried out for specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements by not for profit associations, bodies or organisations, whether recognised or not, of political, philosophical, religious or trade unionist nature, including political parties and movements, with regard to personal data concerning members and/or entities having regular contacts with said associations, bodies or organisations in connection with the aforementioned purposes, provided that the data are not communicated or disclosed outside and the bodies, associations or organisations lay down suitable safeguards in respect of the processing operations performed by expressly setting out the arrangements for using the data through a resolution that shall be made known to data subjects at the time of providing the information under

Section 13 of the Privacy Code

- if the processing is necessary to protect a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted

- if the processing is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefor. Said claim must not be overridden by the data subject's claim, or else must consist in a personal right or another fundamental, inviolable right or freedom, if the data can disclose health and sex life, or

- if the processing is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context, also with regard to occupational and population hygiene and safety and to social security and assistance purposes, to the extent that it is provided for in the authorisation and subject to the requirements of the code of conduct and professional practice referred to in Section 111 of the Privacy Code.

The *Garante* has issued general authorisations for the processing of sensitive data.

TRANSFER

The data controller may freely transfer personal data among the EU Member States. Such transfer can only be prohibited when it is made for the purposes of avoiding the measures that would be applied pursuant to the Privacy Code.

Personal data that is the subject of processing may be transferred from the State's territory to countries outside the European Union, temporarily or not and in any form and by any means whatsoever:

- if the data subject has given his/her consent either expressly or, where the transfer concerns sensitive data, in writing

- if the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject

- if the transfer is necessary for safeguarding a substantial public interest that is referred to by laws or regulations, or else that is specified in pursuance of Sections 20 and 21 of the Privacy Code where the transfer concerns sensitive or judicial data

- if the transfer is necessary to safeguard a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted

- if the transfer is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are transferred exclusively for said purposes and for no longer than is necessary therefor in compliance with the legislation in force applying to business and industrial secrecy

- if the transfer is carried out in response to a request for access to administrative records or for information contained in a publicly available register, list, record or document, in compliance with the provisions applying to this subject-matter, or

- if the transfer is necessary, pursuant to the relevant codes of conduct referred to in Annex A) of the Privacy Code, exclusively for scientific or statistical purposes, or else exclusively for historical purposes, in connection with private archives that have been declared to be of considerable historical interest under Section 6(2) of legislative decree no. 490 of 29 October 1999, enacted to adopt the consolidated statute on cultural and environmental heritage, or else in connection with other private archives pursuant to the provisions made in said codes.

The transfer of processed personal data to a non-EU Member State shall also be permitted if it is authorised by the *Garante* on the basis of adequate safeguards for data subjects' rights:

- as determined by the *Garante* also in connection with contractual safeguards, or else by means of rules of conduct as in force within the framework of companies all belonging to the same group. A data subject may establish his/her rights in the State's territory as set forth by the Privacy Code also with regard to noncompliance with the aforementioned safeguards, or

- as determined via the decisions referred to in Articles 25(6) and 26(4) of Directive 95/46/ EC of the European Parliament and of the Council, of 24 October 1995, through which the European Commission may find that a non EU Member State affords an adequate level of protection, or else that certain contractual clauses afford sufficient safeguards.

It is prohibited to transfer personal data from the State's territory to countries outside the European Union, temporarily or not and in any form and by any means whatsoever, if the laws of the country of destination or transit of the data do not ensure an adequate level of protection of individuals.*

Account shall also be taken to the methods used for the transfer and the envisaged processing operations, the relevant purposes, nature of the data and security measures.

**** Following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. Last 22 October 2015, the Garante declared no longer valid the authorization to transfer personal data in US based on the US-EU safe harbor regime and accordingly prohibited such transfers. The Garante reminds that data transfers to third countries (US included) can still be carried out adopting the Standard Model Clauses or within the framework of the binding corporate rules. Please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the Schrems decision.***

SECURITY

Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorised access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B to the Privacy Code:

- computerised authentication

- implementation of authentication credentials management procedures

- use of an authorisation system
- regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenance of electronic means
- protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software
- implementation of procedures for safekeeping backup copies and restoring data and system availability
- implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

Processing personal data without electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B to the Privacy Code:

- regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of the processing and/or by the individual organisational departments
- implementing procedures such as to ensure safekeeping of records and documents committed to the entities in charge of the processing for the latter to discharge the relevant tasks, and
- implementing procedures to keep certain records in restricted access filing systems and regulating access mechanisms with a view to enabling identification of the entities in charge of the processing.

Certain data controllers must implement further security measures in the framework of certain specific data processing (e.g. processing of biometric data).

BREACH NOTIFICATION

Legislative Decree No. 69/2012 (implementing the Directive 2009/12/EC) amended the Privacy Code provisions in relation to breach notification by introducing:

- the definition of 'personal data breach' (meaning '*a breach of security leading to the accidental destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service*' – Section 4, par. 3, let. g-bis), and
- new obligations in case of personal data breach.

In particular, in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the *Garante*. When the personal data breach is likely to adversely affect the personal data or privacy of a contracting party or other individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification shall not be required if the provider has demonstrated that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

The notification to the contracting party or individual shall at least describe 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. The notification to the *Garante* shall, in addition, describe the

consequences of, and the measures proposed or taken by the provider to address, the personal data breach (Section 32-bis of the Privacy Code).

The *Garante* extended mandatory breach notification requirements in case of data breach relating to processing in the framework of the Electronic Health Record and processing of biometric data.

ENFORCEMENT

The *Garante* is authorised to investigate complaints and to impose sanctions. The *Garante* may also appoint experts, proceed with inspections, require to produce documents and to be granted access. In case of criminal actions, the *Garante* notifies the public prosecutor.

Among others, the Privacy Code provides for the following administrative sanctions:

- providing no or inadequate information to data subjects shall be punished by a fine consisting in payment of between six thousand and thirty six thousand Euro (Section 161 of the Privacy Code)

- processing personal data without the relevant data subject consent (if required) or in breach of the minimum security measures shall be punished by a fine consisting in payment of between ten thousand and one hundred and twenty thousand Euro (Section 162 of the Privacy Code), and
- processing personal data in breach of the decision/ orders issued by the *Garante* shall be punished by a fine consisting in payment of between thirty thousand and one hundred and eighty thousand Euro (Section 162 of the Privacy Code)

- processing personal data without submitting the notification to the *Garante* (if required) shall be punished by a fine consisting in payment of between twenty thousand and one hundred and twenty thousand Euro (Section 163 of the Privacy Code).

Where any of the violations referred to in Sections 161, 162 and 163 is less serious by having also regard to the social and/or business features of the activities at issue, the upper and lower thresholds set forth in the said sections shall be reduced to two-fifths thereof (Section 164-bis, par. 1 of the Privacy Code).

Where one or more provisions mentioned above are violated repeatedly, also on different occasions, in connection with especially important and/or large databases, an administrative sanction shall be applied as consisting in payment of a fine ranging from fifty thousand and three hundred thousand Euro (Section 164-bis, par. 2 of the Privacy Code).

In other, more serious cases, in particular if the prejudicial effects produced on one or more data subjects are more substantial or if the violation concerns several data subjects, the upper and lower thresholds of the applicable fines shall be doubled (Section 164-bis, par.3 of the Privacy Code).

The fines referred above may be increased by up to four times if they may prove ineffective on account of the offender's economic status (Section 164-bis, par. 4 of the Privacy Code).

The Privacy Code also provides for certain criminal sanctions.

ELECTRONIC MARKETING

The Privacy Code (Section 130) does not prohibit the use of personal data for the purpose of electronic marketing, but it requires the prior informed consent (opt-in) from the recipient of the communication. The use of automated calling or communications systems without human intervention for the purposes of direct marketing or for sending advertising materials, or else for carrying out market surveys or interactive business communication, as well as electronic communications performed by e-mail, facsimile, MMS or SMS-type messages or other means shall only be allowed with the contracting party's or user's consent. Such consent shall be recorded with reference to its date and the person giving it in order to be used as evidence of the consent.

Separate consents shall be required for the registration to a website and the opt-in to the delivery of marketing communications, however the data subjects may be required to provide a unique marketing consent covering the different marketing practices (eg marketing via SMS, email, telephone, market surveys, etc.) performed through the collected data, provided that such practices are outlined in the information notice provided to data subjects.

An additional separate consent shall be required for the transfer of collected personal data to third parties for marketing purposes. Said third party shall also be identified at least on the basis of its category of operation and provide an information notice to data subjects before the delivery of marketing communications.

Where a data controller uses, for direct marketing of his own products or services, electronic contact details for electronic mail supplied by a data subject in the context of the sale of a product or service, said data controller may fail to request the data subject's consent, on condition that the services are similar to those that have been the subject of the sale and the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications. The data subject shall be informed of the possibility to object to the processing at any time, using simple means and free of charge, both at the time of collecting the data and when sending any communications for the purposes here referred.

Electronic marketing communications shall clearly identify the sender and provide to the recipient all necessary information in order for him/her to eventually refuse the delivery of the direct marketing material (*opt-out*).

The possibility for the recipient to opt-out from marketing communication services must be guaranteed both during the first contact with the recipient and during any following communications.

Marketing communications by way of non-automated telephone calls are permitted provided that either:

- the data subject has given his prior consent, or
- the number of the data subject is included in the telephone directory and (s)he has not entered in a public opt-out register (*Registro delle Opposizioni*) and opted out from being contacted for marketing purposes.

The above mentioned privacy provisions apply also to communications sent through private messages on social networks and through Voip. On the contrary should the data subject be a follower of a social network page, it may be implied that the data subject has consented to the delivery of marketing communications of the page. Marketing messages concerning a given brand, product or service as sent by the company managing the relevant social network page may be considered to be lawful if it can be inferred unambiguously from the context or the operational arrangements of the relevant social network, also based on the information provided, that the recipient did intend in this manner to also signify his/her intention to consent to receiving marketing messages from the given company. However the delivery of marketing communications shall stop when the data subject unregisters from the page.

Legislative Decree No. 69/2012 (implementing the Directive 2009/12/EC) amended the Privacy Code provisions relating to marketing and commercial communications by making reference to the 'contracting party's and user's consent' rather than to the 'data subject's consent', given that the definition of 'data subject' has been amended so as to include only natural persons and exclude companies from the application of the Privacy Code, with the exceptions of electronic marketing provisions. Indeed, the *Garante* clarified that the provisions of the Privacy Code on marketing obligations still apply to companies as well (and not only to natural persons).

ONLINE PRIVACY

The Privacy Code as amended by Legislative Decree No. 69/2012 (implementing the Directive 2009/12/EC) regulates the collection and processing of traffic data and location data by the provider of a public communications network or publicly available electronic communications service and the use of cookies.

According to Section 123 of the Privacy Code, traffic data shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication. However traffic data can be retained for a period not longer than 6 months for billing and interconnection payments purposes or, with the prior consent of the

contracting party or user (which may be withdrawn at any time), for marketing electronic communications services or for the provision of value added services.

According to Section 126 of the Privacy Code, location data may only be processed if made anonymous or if the subscriber or user has been properly informed and (s)he has given her/ his prior consent (which can be withdrawn at any time).

According to Section 122 of the Privacy Code (which reflects recital 66 of the E-Cookies Directive 2009/136/EC and the amended Section 5, par. 3 of the Directive 2002/58/EC – as amended by Directive 2009/136/EC) the storing of information in the contracting party's or user's computer is only allowed if said contracting party or user has been properly informed and (s)he has given her/his consent.

The Privacy Code states that the *Garante* may determine certain simplified modalities to provide contracting parties or users with the information notice and to identify the most efficient and practical ways to implement the new obligations on cookies. For this purpose, the *Garante* has issued a decision on the "simplified information notice and cookie consent" ("Cookie Decision") in force since June 2015. With the Cookie Decision, the *Garante* clarifies the distinction between technical and profiling cookies. Technical cookies are cookies required for providing "electronic communications or information society services"; in other words, all cookies required to ensure the running of the site. To this broad category, the *Garante* associates also the the functionality cookies to improve the service provided to the users (e.g. language preferences) and analytics cookies placed by the publisher or the manager of the site (editore o gestore del sito), provided that the power of identification of the data processed is reduced and the third party providing analytics services undertakes not to combine such data with other information it may have. Behavioral or profiling cookies are all cookies that allow a profiling of the user, so as to propose to the same user more tailored advertising. All cookies which do not fall under the technical cookies category are subject to the requirements provided for profiling cookies.

While no prior consent is provided for technical cookies, behavioral cookies require a specific and express consent.

The *Garante* clarifies the distinction between first and third party cookies, defining as first party cookies all cookies placed by the publisher or the manager of the site, whereas all third party cookies are simply those cookies that are not placed by the first party. In this respect, the *Garante* acknowledges that the first parties may well not be aware of the existence of third parties placing cookies through the same first parties' site. Consequently, in collecting the consent also for third parties' cookies, the first parties are considered as mere "technical intermediary" (intermediari tecnici). All websites with cookies have to provide for a two layer information notice, with a first summarized notice including a link to a second and more complete notice.

The first simplified notice is set through a banner to be placed in the homepage and any landing page and to be devised in a way to create some "discontinuity" with the usage of the site contents. The banner will also contain some basic information, including a mention of any placing of behavioral or third parties cookies, a link to the extended information notice, the mention that it is possible to deny consent, and the indication that the continuation of the usage of the site will imply a cookie acceptance.

Consent has to be provided through "a positive action", i.e. by removing banner through a click or continuing to read other underlying active pages. It is not possible to simply ignore the banner. The publisher or manager of the site has to keep track of such consent through a (technical) cookie.

The simplified information notice has to link to the more complete information notice, which will include more analytical information, including all information required by the Privacy Code. Such notice has to include also the links to the third parties' information notices, or other intermediary parties. It should also be specifically mentioned the possibility to object against the usage of cookies also through the browser settings.

KEY CONTACTS

Giangiacomo Olivi
Partner
T +39 02 80 618 515
giangiacomo.olivi@dlapiper.com

Giulio Coraggio
Senior Counsel
T +39 02 80 618 619
giulio.coraggio@dlapiper.com

Gianluigi Marino
Associate
T +39 02 80 618 654
gianluigi.marino@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

JAPAN

Last modified 27 January 2016

LAW IN JAPAN

The Act on the Protection of Personal Information ("APPI") requires business operators who utilize for their business in Japan a personal information database which consists of more than 5,000 individuals in total identified by personal information on any day in the past six months to protect personal information. Amendments to the APPI, which were passed in 2015 and go into effect no later than September 2017[1] (the "Amendments"), apply the APPI to all businesses in Japan, regardless of whether the business operator maintains a database of more than 5,000 individuals.

Further, the Amendments clarify the definition of personal information, add two new classes of information, and introduce new requirements for "opt out" choice for business operators to disclosure personal information to third parties. Finally, as of January 1, 2016, the Amendments created a Privacy Protection Commission (the "Commission"), a central agency which will act as a supervisory governmental organization on issues of privacy protection.

[1] The Amendments must be enacted no later than September 2017, so the Amendments could go into effect at an earlier date.

DEFINITIONS

Definition of personal data

Personal information is information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information. Personal Information includes information which enables one to identify specific individual with easy reference to other information.

The Amendments clarify that personal information includes any "personal identifier code", which refers to any biometric data that identifies a specific individual, or any code uniquely assigned to an individual with respect to the receipt of goods or services, or instruments with which to purchase such goods or services.

Definition of sensitive personal data

The Amendments will add a new concept into the APPI: sensitive information. Sensitive information includes information about a person's race, creed, social status, medical history, criminal record, any crimes a person has been a victim of, and any other information that might cause the person to be discriminated against. Obtaining sensitive information generally requires consent from the data subject. Additionally, the "opt out" option (discussed below) is not available for sensitive information--prior consent is required from the party whose sensitive information would be given to a third party

Definition of anonymized information

In addition to sensitive information, the Amendments will add to the APPI the concept of anonymized information. "Anonymized information" refers to any information about individuals from which all personal information (i.e., the

information that can identify a specific individual, including any sensitive information) has been removed and such removed personal information cannot be restored. As noted above, personal information includes personal identifier codes, so these must also be removed before information is considered anonymized. Business operators must ensure that the personal information cannot be restored.

If a business operator has sufficiently anonymized the information, it can be disclosed to third parties without requiring the consent of the individuals whose personal information has been removed from the documents. However, care must be taken in anonymizing the information before disclosure; a failure to completely sanitize the information could result in the disclosure of personal information. Additionally, before disclosing the anonymized information to a third party, a business operator must publicly state (likely in its privacy policy) the nature of information included in the anonymized information, and the means by which it is sharing the anonymized information. Finally, the Commission has been tasked with instituting rules for disclosure, including the standards of anonymization.

NATIONAL DATA PROTECTION AUTHORITY

The Amendments created the Privacy Protection Commission (the "Commission"), which will act as a supervisory governmental organization on issues of privacy protection. The Commission, as noted elsewhere, has also been tasked with providing many of the details necessary to bring the Amendments into effect.

Currently, privacy protection is managed by each of the ministries that supervise the various industries of the private sector. Each of these ministries has adopted its own guidelines for privacy protection, which has led to overlapping and conflicting rules. The Commission is expected to bring these guidelines into alignment.

The Commission will be neutral and independent, and it will have the power to enforce the APPI. It is expected to adopt a more transparent and consistent approach to enforcement than what is currently in place with the various ministries. However, it will only have the right to perform audits and issue cease and desist orders; it will not have the power to impose administrative fines.

REGISTRATION

Japan does not have a central registration system.

DATA PROTECTION OFFICERS

There is no specific legal requirement to appoint a data protection officer. However, some guidelines provide that specific employees should be assigned to control personal data (eg Chief Privacy Officer).

COLLECTION & PROCESSING

Specifying the Purpose of Use

When handling personal information, a business operator must specify to the fullest extent possible the purpose of use of the personal information ('Purpose of Use'). Once a business operator has specified the Purpose of Use, it must not then make any changes to the said purpose which could reasonably be considered to be beyond the scope of what is duly related to the original Purpose of Use. In addition, when handling personal information, a business operator shall not handle the information beyond the scope that is necessary for the achievement of the Purpose of Use without a prior consent of the individual. In other words, the use of the information must be consistent with the stated Purpose of Use.

Public Announcement of the Purpose of Use

The Purpose of Use must be made known to the individual when personal information is collected or promptly thereafter and this can be made by a public announcement (such as posting the purpose on the business operator's website). When personal information is obtained by way of a written contract or other document (including a record made in an electronic or magnetic format, or any other method not recognisable to human senses), the business operator must expressly state the Purpose of Use prior to the collection.

A business operator must ‘publicly announce’ or ‘expressly show the Purpose of Use’ in a reasonable and appropriate way. According to the ‘Guidelines for the APPI Concerning Fields of Economy and Industry’ issued by the Ministry of Economy, Trade and Industry ('METI Guidelines'), the most appropriate method for a website to publicly announce the Purpose of Use of information collected, is a one click access on the homepage.

TRANSFER

Disclosing/Sharing Personal Data

Currently, personal data may not be disclosed to a third party without the prior consent of the individual, unless permitted by the exceptions under the APPI. Even disclosing the data within group companies is considered disclosing the data to a third party and consent must be obtained, unless it meets the requirements of joint use. The APPI also has permitted the "opt out" method, whereby a business operator can as a default disclose personal information to third parties, unless individuals opt out of allowing the business operator to do so, however the Amendments newly require a business operator to notify the Committee of certain items concerning opt out.

The APPI does not provide any examples of how best to obtain consent from individuals before sharing information. Generally, written consent should be obtained whenever possible. When obtaining consent it would be prudent to clearly disclose to the individual the identity of the third party to whom the personal data will be disclosed, the contents of the personal data and how the third party will use the provided personal data.

If personal data is to be used jointly, the business operator collecting the information could, prior to the joint use, notify the individuals providing the personal information of the following:

- the fact that the personal data will be used jointly
- the scope of the joint users
- the purpose for which the personal data will be used by them, and
- the name of the individual or business operator responsible for the management of the personal data.

The current METI Guidelines provide the following examples as appropriate methods of obtaining the consent for disclosing personal data from the individual:

- receipt of confirmation of the oral or written consent (including a record created by electronically or magnetically methods or any other method not recognizable to human senses) from such person
- receipt of a consent email from such person
- the person's check of the confirmation box concerning the consents
- the person's click of a button on the website concerning the consents, and
- the person's audio input, or touch of a touch panel concerning the consents

With the Amendments, a business operator will be able to disclose personal data to a third party without the individual's consent, so long as the following are publicly disclosed:

- the purpose of use includes the provision of such information to third parties;
- the nature of the personal data being provided to third parties;
- the method by which personal data is provided to third parties;
- the matter that provision of such information to third parties will be stopped upon the request by the data subject; and

- the method for an individual to submit an opt out request to the company.

If the individual does ask to opt out, the business operator must comply with this request. In addition to the public disclosure requirements, a business operator must provide advance notification to the Commission that it is doing so. Additionally, if the business operator changes the nature of the personal data being provided to a third party or the means by which it is providing the personal data, it must notify the Commission of the changes. The Commission will publicly disclose the notification.

Cross-border Transfer

Under the amended APPI, in addition to the general requirements for disclosure or joint use, prior consent of individuals specifying the receiving country is required for transfers to third parties in foreign countries except if the transfer is to (i) a receiver having a data protection system which is equivalent to the system required under the APPI, or (ii) a receiver located in a country that is designated by the Committee as providing an adequate level of protection. The details of requirements for (i) and (ii) are to be determined by the Committee.

SECURITY

The APPI requires that business operators prevent the leakage of personal data. The APPI does not set forth specific steps that must be taken. Ministry guidelines impose specific steps that business operators should take to ensure that personal data is secure. These necessary and appropriate measures generally include 'Systematic Security Control Measures', 'Human Security Control Measures', 'Physical Security Measures' and 'Technical Security Control Measures'.

Guidelines often contain several specific steps or examples that entities subject to the Guidelines must take with respect to each of the security control measures such as developing internal guidelines pertaining to security measures, executing non-disclosure contracts with employees who have access to personal data, protecting machines and devices and developing a framework to respond to instances of leakage.

BREACH NOTIFICATION

The APPI does not explicitly require notification to a ministry or governmental authority in the event of a leak or security breach that may lead to a leak of personal data, although a ministry may request that a report be submitted.

However, the JFSA Guidelines provide that a business operator regulated by the JFSA must immediately produce a report when a leakage of personal information occurs. In addition, the business operator must promptly publicise the facts related to the leakage and the steps taken to prevent the reoccurrence of similar event. Finally, the JFSA Guidelines require that the business operator notify the individual whose information has been leaked of the leakage.

The current METI Guidelines provide suggested measures that business operators, subject to the Guidelines, should take if there is a leak or breach of security with respect to personal data.

The current METI Guidelines' measures include the following:

- a business operator should notify the individuals whose personal data may have been compromised, although there may be circumstances where notifying individuals may not be necessary depending on the specific facts. Relevant factors to consider are the harm (including potential harm) to the individuals concerned

- a business operator should voluntarily file a report of the incident with METI. METI will potentially make such reports public, and

- a business operator should make public the nature of the incident, the steps taken to ensure that it does not happen again.

ENFORCEMENT

Enforcement of the APPI is currently handled by the minister with jurisdiction over the business of the business operator, and the Minister of Health, Labor and Welfare with respect to the employment.

The minister may:

- require an business operator to submit reports regarding the handling of personal information
- provide necessary advice to the business operator with respect to the entity's handling of personal information
- recommend a business operator to cease violations or correct violations of the specific provisions of the APPI, and
- order a business operator to take the recommended or necessary measures.

If the business operator does not provide a report as required by a minister or has made a false report the business operator is subject to a fine of up to JPY300,000. If the business operator fails to follow a corrective order by a minister, the business operator is subject to a fine of up to JPY300,000 or imprisonment with work of up to six months. In addition, the entity shall be sentenced to the fine if an officer or an employee of the entity commits any of the above violation concerning the business of the entity.

The Commission will take over the power to enforce the APPI after the Amendments come into force. Although, it has the right to perform audits and inspections against business operators and to issue cease and desist orders; it does not have the power to impose administrative fines.

Finally, the Amendments will add a criminal penalty provision to the APPI. An unauthorized disclosure of personal information, for the benefit of the disclosing party or any third party, will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY500,000. If the party making the disclosure is a legal entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure.

ELECTRONIC MARKETING

The Act on Specified Commercial Transactions ('ASCT') and the Act on the Regulation of Transmission of Specified Electronic Mail ('Anti-Spam Act') regulate the sending of unsolicited electronic commercial communications.

Under the ASCT, which focuses on internet-order services and mail-order services, a seller is prohibited from sending email advertisements to consumers unless they provide a prior request or consent (ie an opt-in requirement). The seller is also required to retain the records that show consumers' requests or consents to receive email advertisements for 3 years after the last transmission date of an email advertisement to the consumer.

If a seller has breached any of these obligations, such seller will be potentially subject to fine of up to JPY 1,000,000.

Under the Anti-Spam Act, which broadly covers commercial emails (eg an invitation email from a social network service), there are several regulations on sending email advertisements as follows:

- the sender must retain records evidencing there was a request or consent to receive emails at least for 1 month after the last date the seller sent an email to the recipient
- for-profit entities or individuals engaged in business sending any email to advertise their own or another's business must obtain a request or consent to receive emails from intended recipients unless the recipient falls under certain exceptions (eg there is a continuous transaction relationship between a sender and a recipient) in the Anti-Spam Act
- an email is required to include a sender's email address or a URL so that recipients can send opt-out notices to

the sender, and

- senders must not send emails to randomly generated email addresses (with the hope of hitting an actual email address) for the purpose of sending emails to a large number of recipients.

The relevant ministry may order a sender to improve the manner of email distribution if the sender violates the requirements noted above. If the sender violates an order issued by the ministry (other than one related to the retention obligation), the sender is subject to imprisonment for up to 1 year or a fine of up to JPY 1,000,000. The entity will be subject to fine of up to JPY 30,000,000 if an officer or an employee of the entity commits any violation mentioned above. If the sender violates an order issued by the minister with respect to the retention obligation, the sender will be potentially subject to fine of up to JPY 1,000,000.

ONLINE PRIVACY

There is no law in Japan that specifically addresses cookies and location data. However, if the information obtained through cookies may identify a certain individual in conjunction with other easily-referenced information (eg member registration) and it is utilised (eg for marketing purposes), such Purpose of Use of information obtained through the use of cookies must be disclosed under the APPI. METI takes the same position in its guidelines.

KEY CONTACTS

Lawrence G. Carter
Partner
T +81 3 4550 2800
lawrence.carter@dlapiper.com

Keitaro Uzawa
Associate
T +81 3 4550 2800
keitaro.uzawa@dlapiper.com

Brian Caster
Associate
T +81 3 4550 2800
brian.caster@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

JERSEY

Last modified 27 January 2016

LAW IN JERSEY

The Data Protection (Jersey) Law 2005 ('Law) came into force on 1 December 2005.

Jersey's data protection legislation has been held to be adequate by the European Commission for the purposes of the European Data Protection Directive (Directive 95/46/EC) (see Commission Decision 2008/393/EC).

DEFINITIONS

Definition of personal data

'Personal data' is defined under the Law as data relating to a living individual who can be identified:

- from the data, or
- from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Definition of sensitive personal data

'Sensitive Personal Data' is defined under the Law as personal data relating to:

- the racial or ethnic origin of the data subject
- the political opinions of the data subject
- the data subject's religious beliefs or other beliefs of a similar nature
- whether the data subject is a member of a trade union
- the data subject's physical or mental health or condition
- the data subject's sexual life
- the data subject's commission, or alleged commission, of any offence, and
- any proceedings for any offence committed, or alleged to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in any such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Information Commissioner
Brunel House
Old Street
St.Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
E: enquiries@dataci.org

REGISTRATION

Data controllers who process personal data must inform the Information Commissioner (an online portal is available) of the following:

- the name and address of the data controller (including a Jersey resident representative if the data controller is outside Jersey)
- a description of the personal data being, or to be, processed by or on behalf of the data controller and of the category or categories of data subject to which they relate
- a description of the purpose or purposes for which the data are being or are to be processed
- a description of the recipients (if any) to whom the data controller intends or may wish to disclose the data, and
- the names, or a description, of any countries or territories outside Jersey to which (directly or indirectly) the data controller transfers, or intends or may wish to transfer, the data.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer in Jersey.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject consents
- the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party
- the processing satisfies the data controller's legal obligation
- the processing protects the data controller's vital interests
- the processing is required by an enactment, the Crown or the government
- the processing is required to perform a public function in the public interest, or to administer justice, or
- the data controller has a legitimate reason for the processing, except if the processing would damage the data subject's rights, freedoms or other legitimate interests.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of additional conditions.

The data controller must provide the data subject with "fair processing information". This includes the identity of the data

controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

The Law provides that data controllers may transfer personal data out of the European Economic Area if any of the following conditions are met:

- the data subject consents
- the transfer is essential to a contract to which the data subject is party
- the transfer is needed to carry out a contract between the data controller and a third party if the contract serves the data subject's interests
- the transfer is legally required or essential to an important public interest
- the transfer protects the data subject's vital interests, or
- the data is public.

Transfers of personal data to jurisdictions outside of the European Economic Area are allowed if the jurisdiction provides 'adequate protection' for the security of the data, or if the transfer is covered by 'standard contractual clauses' approved by the European Commission. It is likely that Binding Corporate Rules would satisfy the Law.

Following the decision of the Court of Justice of the European Union in Schrems v Data Protection Commissioner (C36214), the US/EU "Safe Harbour" regime is no longer regarded as a valid basis for transferring personal data to the US. Whilst Jersey is not a member of the EU, it can (and does) adopt measures prescribed by the EU in certain areas such as data protection. Jersey uses the EU "adequacy" benchmark to assess whether transfers can be validly made to other jurisdictions.

The Safe Harbour regime had been relied upon as a mechanism for the transfer of data to the US, which did not otherwise have "adequate" measures in place to protect personal data. Now that the regime has been abolished, Jersey businesses are reviewing their procedures. Whilst the Commissioner has not adopted any formal stance in response to the Schrems decision, she is maintaining a close dialogue with the Channel Islands' Brussels office and the UK's Information Commissioner's Office. Whilst awaiting the revised version of the Safe Harbour Privacy Principles, the Commissioner has confirmed that Jersey's existing statutory regime will be adhered to, confirming that she retains the power to investigate complaints made to her, including those founded on transfers reliant upon Safe Harbour as a basis for their validity.

It is anticipated that the Commissioner will likely await the outcome of the US/EU negotiations; however with the prospect of data protection authorities around Europe adopting varying stances, the immediate future remains uncertain. It remains important for businesses to review their procedures and adopt alternative mechanisms if they had previously relied on Safe Harbour.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data.

BREACH NOTIFICATION

There are no specific duties to inform the Data Protection Commissioner of breaches. However, best practice is likely to be (following the UK) to inform the Data Protection Commissioner of a breach where a significant number of data subjects are affected or where significant harm may (or has already) occurred.

ENFORCEMENT

In Jersey, the Information Commissioner is responsible for the enforcement of the Law. This is a dual role which combines the statutory office of Data Protection Commissioner under the Law with the office of Information Commissioner for the purposes of the Freedom of Information (Jersey) Law 2011.

If the Information Commissioner becomes aware that a data controller is in breach of the Law, an enforcement notice may be issued requiring the data controller to rectify the position.

Failure to comply with an enforcement notice is a criminal offence and can be punished with an unlimited fine.

ELECTRONIC MARKETING

The Law will apply to most electronic marketing.

ONLINE PRIVACY

The 2011 amendments implemented by the UK in relation to cookies have not found their way into Jersey law and there are no immediate plans for this to be done, however the Law will generally apply.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Huw Thomas
Counsel
T +44 1534 888900
huw.thomas@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

LATVIA

Last modified 25 January 2016

LAW IN LATVIA

Latvia has implemented the EU Data Protection Directive and the EU Directive on Privacy and Electronic Communications through the Personal Data Protection Law (last amended on 7 March 2014) and the Law on Electronic Communications (last amended on 22 October 2015).

There are also specific rules for electronic documents, biometrics, medical services, debt collections services, e-commerce and telecommunications which provide stronger protection for the personal data subject.

DEFINITIONS

Definition of personal data

The Personal Data Protection Law defines personal data as any information related to an identified or identifiable natural person.

Definition of sensitive personal data

Sensitive personal data personal data which indicate:

- the race
- ethnic origin
- religious
- philosophical or political convictions
- or trade union membership of a person
- or provide information as to the health or sexual life of a person.

NATIONAL DATA PROTECTION AUTHORITY

Data State Inspectorate

Blaumana Street 11/13 11
Riga
LV 1011
Latvia Phone: +371 67 223 131
Fax: +371 67 223 556

E mail: info@dvi.gov.lv

Office hours

Mon 8 12; 12.30 17.00
Tue 8 12; 12.30 17.30
Wed 8 12; 12.30 16.30
Thu 8 12; 12.30 16.30
Fri 8 12; 12.30 15.00

REGISTRATION

There is no obligation to register with the Data State Inspectorate ('DSI') before starting data processing unless the intent is:

1. to transfer personal data to a state outside EU and EEA
2. to process personal data when providing financial or insurance services, carrying out raffles or lotteries, market or public opinion researches, personnel selection or personnel assessment as the form of commercial activity, when providing debt recovery services and credit information processing services as the form of commercial activity
3. to process sensitive personal data (with the exception in cases when sensitive personal data are processed for the purposes of accounting, within employment relationship or by religious organisations)
4. to processes personal data in relation to the criminal offences, criminal records and penalties in administrative violations matters
5. to carry out video surveillance and retain such data
6. to process genetic (biometric) data of the person.

If the person intends to process the data which requires prior registration with the DSI, it is permitted not to register with the DSI if a personal data protection specialist (a natural person having required qualification) is assigned. In that case the personal data protection specialist must be registered with DSI indicating his/her contact information, the place of data processing and the term of his/her assignment.

If for intended data processing activities the registration is required and data protection specialist will not be appointed, then the data controller has to register with DSI by using a standard form, which includes information about:

- the name and contact details of the data controller
- the name and contact details of data controller's representative (if any)
- the legal basis for the processing of personal data
- the list of categories of personal data that are being processed
- the purpose of the data processing
- the categories of data subjects
- the categories of recipients of personal data
- the intended method of processing of personal data
- the planned method of obtaining personal data
- the place of processing of personal data
- the holder of information resources or technical resources, as well as a person responsible for the security of the information system
- technical and organisational measures ensuring the personal data protection
- the type of personal data to be transferred outside EU/EEA.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a data protection officer (defined as a personal data protection specialist under the Personal Data Protection Law). However, a data controller is exempt from registering data processing activities with DSI if the data controller has appointed a data protection officer ('DPO').

The appointed DPO has the obligation to organise, control and supervise the compliance of data processing with the legal requirements. The DPO keeps a register with data and upon request of data subject or DSI it must disclose the

information about:

- the name and contact details of the data controller
- the name and contact details of data controller's representative (if any)
- the legal basis for the processing of personal data
- the list of categories of personal data that are being processed
- the purpose of the data processing
- the categories of data subjects
- the categories of recipients of personal data
- the intended method of processing of personal data
- the planned method of obtaining personal data
- the place of processing of personal data
- the holder of information resources or technical resources, as well as a person responsible for the security of the information system
- technical and organisational measures ensuring the personal data protection
- the type of personal data to be transferred outside EU/EEA.

COLLECTION & PROCESSING

The Personal data protection law defines data processing as any operations carried out regarding personal data, including data collection, registration, recording, storing, arrangement, transformation, using, transfer, transmission and dissemination, blockage or erasure. According to the Personal Data Protection Law personal data may be processed only if:

- the data subject has given his consent
- a contract to which the data subject is party is being concluded or performed
- it is a legal obligation of the data controller under laws to process personal data
- processing is necessary in order to protect vital interests of the data subject
- processing is necessary for the exercise of official authority vested by laws and other legal acts in state and municipal institutions, agencies, enterprises or a third party to whom personal data are disclosed
- processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data is disclosed, unless such interests are overridden by interests of the data subject.

Moreover, the data controller has to ensure that:

- all personal data is processed fairly and lawfully
- all personal data is collected for specific, explicit and legitimate purposes and are subsequently processed in accordance with these purposes
- all personal data collected is adequate, relevant, and non excessive in view of the purposes for which they are collected
- all personal data is accurate, comprehensive and, when necessary, kept up to date
- all personal data is retained for no longer than is necessary for the purposes for which it is processed.

For the processing of sensitive personal data further restrictions apply. Where sensitive personal data is processed, a different, exhaustive list of specific conditions applies. With regard to sensitive data, the legitimate interest in confidentiality will not be infringed in the following circumstances:

- where the data subject has given explicit consent to the use of the data
- where the use of the data without obtaining consent is authorised or required by labour or employment law, regulating the protection of such personal data
- where processing or disclosure is necessary to safeguard the vital interests of the data subject, and the data subject is legally or physically unable to give consent
- where data is necessary to reach the non commercial goals of non profit organisations and such data related to the scope of their activities and members and such data are not disclosed to third persons
- where the use of the data is required for medical prevention, medical diagnostics, health care or treatment, or for the administration of medical services
- where the use of the data is necessary for the enforcement, exercise or protection of persons legal interests at court
- where the use of the data is required for the provision of social assistance and it is performed by the provider of social assistance services
- where the use of the data is necessary for the establishment of the national documentary heritage and it is performed by the Latvian national archives and accredited private archives
- where the processing of the data is necessary for statistical research, which is performed by the Central Statistics Bureau
- where the data was clearly made public by the data subject
- where the processing of the data is necessary when performing state administration functions or establishing state information systems laid as required by law
- where the data is necessary when the person is claiming the indemnity in accordance with the insurance contract
- where the patient's data recorded in medical documents are used in a research in conformity to the Law On the Rights of Patients.

TRANSFER

Personal data may be transferred to another state if that state ensures the same level of data protection as is in effect in Latvia. There are no restrictions on data transfers inside the EU and EEA as well as in a few other countries – a list accepted by the European Commission and the DSI (the so called 'white list').

Transfer to other jurisdictions is permissible if the data controller would perform supervision regarding the performance of the relevant protection measures in compliance with Latvian law, ie written data transfer agreement is needed, or at least one of the following conditions is fulfilled:

- the express consent of the data subject for the transfer is obtained
- the transfer of the data is necessary to fulfil an agreement between the data subject and the data controller, the transfer is needed for data subject's contractual obligations or the data subject has requested the transfer in order to enter into a contract
- when there is a significant state or public interest, or the transfer is required for judicial proceedings
- the transfer of the data is necessary to protect the life and health of the data subject

- if transferable, the data is public or has been accumulated in a publicly accessible register.

The DSI will grant its approval if, in the specific case, adequate protection can be evidenced. This may be achieved by:

- including terms and conditions in the written agreement that are provided in the Cabinet of Ministers Regulations No 634 of 16 August 2011 'Terms for mandatory provisions to be included in personal data transfer agreements'
- If data controller ensures that it is bound by Corporate Rules
- by including EU model clauses in the written agreement.

In any case, prior to transferring data outside the EU/EEA the relevant data processing activities need to be registered with the Data State Inspectorate, unless the data controller has not previously appointed and registered with the Data State Inspectorate a personal data protection specialist

SECURITY

Under Personal Data Protection Law it is the obligation of the data controller and processor to implement appropriate technical and organisational measures, depending on the technological state of the art and the cost incurred in execution, to protect personal data against accidental or intentional destruction or loss, unauthorised disclosure or access and against all other unlawful forms of processing.

The law does not contain a list of specific measures to be adopted by data controller or processor. However in 2014 DSI has published guidelines 'Security of personal data processing' where it lists various measures (eg anti virus software, password protection, data encryption, regular trainings of the employees, etc) that would increase the security and ensure adequate level of protection.

BREACH NOTIFICATION

Breach notification

The Electronic Communications Law provides the obligation for the providers of electronic communications services to immediately notify the DSI about the occurred breach of security. Within 30 days from the notification, the provider of electronic communications services must inform the DSI about:

- the types of personal data, categories of data subjects and data amount in respect of which personal data protection breach has occurred
- technical and organisational protection measures and means that were in place at the moment of the breach
- the measures taken to mitigate the consequences of the breach
- the consequences of the breach
- technical and organisational measures implemented after the breach
- carried investigation of the breach
- any third persons that are informed of this breach
- the fact whether the data subjects in respect of which the breach of personal data protection has occurred have been informed thereof.

Other data controllers that are not providers of publicly available electronic communications services do not have an obligation to notify individuals or DSI of the occurred data security breach.

Mandatory breach notification

The providers of publicly available electronic communications services have the mandatory obligation to notify DSI about the personal data security breach. No other data controllers or processors have this obligation.

ENFORCEMENT

The violation of data protection rules or breach of the rights of data subject is punishable offence under Latvian Administrative violations code. For the data processing without registration (if required) the DSI may impose fine up to EUR 11,000 with or without the confiscation of the objects used to commit the violation.

For not providing information to the DSI or to the data subject, or for providing false information a fine up to EUR 7,100 may be imposed.

For illegal actions with personal data (including collecting, organising, classifying, editing, storing, using, transferring, disclosing, blocking or erasing of the personal data) a fine up to EUR 11,400 with or without the confiscation of the objects used to commit the violation may be imposed. If the offence is committed with regard to sensitive data or repeatedly a fine up to EUR 14,000 may be imposed.

In addition, the individual affected by the breach of the Personal Data Protection Law is also entitled to claim a 'due compensation' which may include pecuniary and moral damages.

There are some criminal sanctions established for unlawful actions with personal data if it has caused serious harm, has been done by the controller or processor with the purpose of blackmailing, with a purpose to gain monetary benefit or for the revenge. However, with respect to usual data processing activities these are enforced in extremely rare cases.

ELECTRONIC MARKETING

The Personal Data Protection Law does not specifically address (electronic) marketing. However the use of personal data for marketing purposes falls within the scope of the law. The provisions on electronic marketing are also included in the Law On Information Society Services, which requires prior express consent of the person before using his/her contact information (eg e mail address, phone number) for electronic marketing purposes. This is also stressed in the guidelines provided by DSI.

According to the provisions of the Law On Information Society Services no consent is required if the data has been obtained in the course of the sale of goods or provision of services, occurs for the same or similar goods or services, the recipient is able to decline easily and with no costs for the use of his/her personal data and the recipient has not previously declared that he or she does not want to be contacted.

ONLINE PRIVACY

Specific issues of online privacy are regulated in the Electronic Communications Law and the Law on Information Society Services.

The Law on Information Society Services states that the storage of information received, including cookies or similar technologies, is permitted, provided that the consent of the person has been received after he or she has received clear and comprehensive information regarding the purpose of intended storage and data processing. Therefore with regard to cookies Latvian law supports an opt in approach.

As to location data, the Electronic Communications Law permits the processing of location data only to ensure the provision of electronic communications services or if the express prior consent is obtained. Moreover, the person whose location data is being processed has the right to revoke his/her consent or to suspend it at any time, notifying the relevant electronic communications merchant of this revocation or requested suspension.

The processing of location data for other purposes without the consent of a user or subscriber is permitted only if it is not possible to identify the person utilising such location data or if the processing of location data is necessary for the Emergency services.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kaupo Lepasepp
Partner
T +372 6 400 900
kaupo.lepasepp@sorainen.com

Mihkel Miidla
Senior Associate, Head of Technology & Data Protection
T +372 6 400 959
mihkel.miidla@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

LESOTHO

Last modified 27 January 2016

LAW IN LESOTHO

The Constitution of the Kingdom of Lesotho guarantees a right to privacy.

The Data Protection Act, 2011 ('Act') was promulgated in 2012 and provides for the principles for regulation of the processing of personal information in order to protect and reconcile the fundamental and competing values of personal information.

DEFINITIONS

Definition of personal data

Personal data or information means data which relates to a living individual who can be identified:

- from that data, or
- from that data and other information which is in the possession, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual.

Definition of sensitive personal data

The Act does not contain an express definition of 'sensitive personal data' but does state that unless specifically permitted under this Act, a data controller shall not process personal information concerning a:

- child who is subject to parental control in terms of the law
- data subject's spiritual, religious or philosophical beliefs, race or ethnic origin, trade union membership, political affiliation, health, sexual life, or criminal behaviour.

NATIONAL DATA PROTECTION AUTHORITY

The Act introduces and provides for the establishment of an independent supervisory authority, namely the Data Protection Commission ('Regulator') specifically established for the purpose of data protection.

REGISTRATION

A data controller shall process personal information only upon notification to the Commission.

DATA PROTECTION OFFICERS

The Act does not provide for the appointment of data protection officers.

COLLECTION & PROCESSING

Personal information may be processed if:

- the data subject provides explicit consent to the processing
- processing is necessary for the conclusion or performance of a contract to which the data subject is a party
- processing is necessary for compliance with a legal obligation to which the data controller is subject
- processing is necessary to protect the legitimate interest of the data subject
- processing is necessary for the proper performance of a public law duty by a public body
- processing is necessary for pursuing the legitimate interest of the data controller or of a third party to whom the information is supplied.

Personal information may only be collected directly from the data subject except under the following circumstances:

- the information is in a public record
- the data subject has consented to the collection from another source
- collection of the information from another source would not prejudice a legitimate interest of the data subject
- collection of the information is necessary:
  - to avoid prejudice to the maintenance or enforcement of law and order
  - for the conduct of proceedings in any court of tribunal
  - in the legitimate interest of national security
  - to maintain the legitimate interest of the data controller or third party.
- compliance would prejudice a lawful purpose of the collection
- compliance is not reasonably practicable in the circumstances of the particular case.

TRANSFER

A data controller shall not transfer personal information about a data subject to a third party who is in a foreign country unless:

- the recipient is subject to a code or law which upholds substantially similar principles for the reasonable processing of information to those principles found in the Act, and includes provisions on transfer restrictions that are similar to those as contained in the Act
- the data subject consents to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the data controller
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject
- the transfer is for the benefit of the data subject.

SECURITY

No particular requirements.

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an (un)authorised person, the data controller, (or any third party processing personal information under the authority of a data controller), is required to notify both the Commission and the data subject, (unless the identity of such data subject cannot be established).

This notification must be made as soon as reasonably possible after the discovery of the breach.

However, the data controller shall delay notification to the data subject where the Lesotho Mounted Police Service, the National Security Service or the Commission determines that notification will impede a criminal investigation.

The notification to a data subject shall be in writing and communicated to the data subject in one of the following ways:

- mailed to the data subject's last known physical or postal address
- sent by e-mail to the data subject's last known e-mail address
- placed in a prominent position on the website of the party responsible for notification
- published in the news media
- as may be directed by the Commission.

A person making notification shall ensure that the notification provides sufficient information to allow the data subject to take protective measures against potential consequences of the compromise, including, if known to the data controller, the identity of the unauthorised person who may have accessed or acquired the personal information.

Mandatory breach notification

See above.

ENFORCEMENT

The Commissioner is empowered to investigate complaints and also to initiate proceedings against a data controller.

A data subject may also institute civil action for damages in a court having jurisdiction against a data controller for breach of any of the provisions of the Act.

ELECTRONIC MARKETING

A data subject is entitled to at any time by notice to a data controller to require the data controller to cease or not to begin, processing or personal data for the purpose of direct marketing. However, there are the specific reasons regarding electronic markets.

The Commissioner is also empowered to take such steps necessary to order the data controller to comply with such notice.

ONLINE PRIVACY

This online privacy is not subject to any express regulation.

KEY CONTACTS

Cliffe Dekker Hofmeyr Inc.
www.cliffedekkerhofmeyr.com

Simone Gill
Director
T +27 (0)11 562 1249
simone.gill@cdhlegal.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

LITHUANIA

Last modified 27 January 2016

LAW IN LITHUANIA

As a member of the European Union, Lithuania has implemented the EU Data Protection Directive 95/46/EC. Lithuania passed the Law on Legal Protection of Personal Data on 11 June 1996 (**Data Protection Law**), which has been amended on 17 July 2000, 22 January 2002 and 21 January 2003 in order to transpose the provisions from the Directive. The latest modifications to the Data Protection Law came into force on 1 September 2011. They include amendments and new regulations on public polls, credit referencing agencies and public governance of data protection. Enforcement is carried out by the State Data Protection Inspectorate (**DPI**).

In addition, Lithuania has fully transposed the Directive 2006/24/EC (the Data Retention Directive) into national law through the Law on Electronic Communications dated 15 April 2004 (**Electronic Communications Law**, latest amendments came into force on 1 August 2011). The Electronic Communications Law protection of privacy in the area of electronic communications.

Please note that the data retention requirements (6 months in Lithuania) were transposed into the relevant local laws from the Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks) which was declared invalid by the CJEU by its decision of 8 April 2014 (Judgment in Joined Cases C-293/12 and C-594/12). However, local laws in Lithuania have not been amended yet, and it is still unclear as to when changes in the legislation will be introduced.

The DPI has issued only a limited number of guidelines on particular data protection issues. Opinions and recommendations of the EU Article 29 Data Protection Working Party are often followed by the DPI and Lithuanian courts while interpreting abstract provisions of the Data Protection Law.

DEFINITIONS

Definition of personal data

Any information relating to a natural person (i.e. data subject) who is known or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his physical,

physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

In the Data Protection Law, sensitive personal data is called “special categories of personal data”.

Special categories of personal data is data concerning racial or ethnic origin of a natural person, his political opinions or religious, philosophical or other beliefs, membership in trade unions, and his health, sexual life and criminal convictions.

NATIONAL DATA PROTECTION AUTHORITY

The State Data Protection Inspectorate (*Valstybinė duomenų apsaugos inspekcija* in Lithuanian, website available here http://ada.lt/)

Address:

A. Juozapavičiaus str. 6/Slucko str. 2

LT-09310 Vilnius Lithuania

T +370 5 279 1445

F +370 5 261 9494

ada@ada.lt

REGISTRATION

Data controllers must notify the DPI about processing of personal data by automated means unless one of the statutory exceptions applies. On the basis of this notification the DPI enters the data controller into the State Register of Personal Data Controllers.

The Data Protection Law establishes the requirement that such data processing may be carried out only when the data controller or his representative notifies the Inspectorate except cases where personal data is processed:

1. for the purposes of internal administration (including group level administration);
2. for political, philosophical, religious or trade union related purposes by a foundation, association or any other non profit organisation on the condition that the personal data processed relates solely to the members of such organisation or to other persons who regularly participate in its activities in connection with the purposes of such organisations;
3. by the media for the purpose of providing information to the public for artistic and literary expression, or
4. in accordance with regulation on state secrets and official secrets.

“Internal administration” covers activities which ensure independent functioning of the data controller: administration, personnel management, management and use of property, financial recourses, clerical work, etc. DPI interprets internal administration only as the activities of data controllers that are necessary, inevitable and stemming directly from statutory requirements. Any other activity/data processing which does not directly derive from the law and is carried out at the initiative of the data controller is considered exceeding the purpose of

internal administration and needs to be notified (for e.g. operating a whistleblowing system, hotline, internal IT helpdesk, etc.).

The data controller when notifying the Inspectorate of data processing has to submit a standard notification form, which includes information about:

1. the purpose of the data processing
2. the groups of data subjects
3. the sources of the personal data
4. the groups of the receivers of the data
5. the list of categories of personal data that are being processed
6. the personal data transfers to foreign countries
7. the personal data retention period
8. the data processors, and
9. the list of security measures.

The DPI has 30 calendar days to adopt its decision. There is no stamp duty. Along with the notification data controller is required to submit a description of data security measures which is a standard form document approved by the DPI.

There are no periodical renewal obligations. However, the registrations should be periodically reviewed internally to make sure they reflect actual situation and the needs of the company.

There are no changes with respect to the prior checking procedure.

DATA PROTECTION OFFICERS

Under the legislation of Lithuania the organisations (data controllers) have a right (but not an obligation) to designate a person to be responsible for the data protection ('Data Protection Officer'). The data controller must notify the Inspectorate of appointment or withdrawal of the data protection officer within 30 days.

In addition, if no data protection officer is appointed, the CEO of the data controller will be *ex officio* deemed responsible for data protection compliance and will be also personally liable for any legal violations of the Data Protection Law.

COLLECTION & PROCESSING

Personal data processing must have a legitimate basis. A legitimate basis under the Data Protection Law, among other things, can be the consent of the data subject, and the legitimate interests of the data controller or by a third party to whom the personal data is disclosed, unless such interests are overridden by interests of the data subject (other criteria for legitimate processing of personal data would most likely be inapplicable in this case).

Data controller must process the personal data lawfully and honestly, and only in conformity with the intended purpose

and not more than to the extent required. Therefore the categories of personal data must be carefully examined and excluded from processing, if their processing is not necessary for the intended purpose

TRANSFER

Transfers within EU/EEA member countries from Lithuania can be carried out without any additional notification or authorisation of the DPI on the basis of a data transfer agreement.

Transfers outside EU/EEA member countries from Lithuania must be prior authorised by the DPI unless one of the statutory exceptions apply (the exceptions include data subject's consent, necessary for implementation of contract, protection of vital interests of data subject, investigation of criminal activity, etc.). The DPI authorises data transfer to third countries if the applicant demonstrates that the recipient country ensures adequate level of protection for personal data. After the *Schrems* decision adequate level of protection can be supported either by providing the DPI with the SCC approved by the European Commission concluded between the data importer and data exporter or by BCR (i.e. Intra-group Data Transfer Agreement) along with the request for authorisation for transfer.

The DPI has 2 months to adopt its decision. There is no stamp duty. There are no periodical renewal obligations. However, the authorisations should be kept up to date.

Same rules apply with respect to transfers of sensitive personal data. Only direct processors (not sub-processors) must be filed with the DPI.

SECURITY

Lithuanian data protection legislation obliges the data controller and data processor to implement appropriate organisational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing. Moreover, they must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc) in accordance with the general requirements on the organisational and technical data protection measures laid down by the Inspectorate. Key measures taken shall be disclosed to the Inspectorate through the data controller registration form.

Specific data security requirements are set forth by General Requirements for Organisational and Technical Data Security Means approved by Order No 1T-71(1.12) of 12 November 2008 of the Director of the Inspectorate.

BREACH NOTIFICATION

In practice, the DPI seldom initiates investigations without a complaint from a data subject or other interested party.

Under the Electronic Communications Law, publicly available electronic communications services providers must notify the DPI of any personal data breach without delay. The provider must also notify the individual of such breach where it is likely to adversely affect their personal data or privacy.

There is no statutory requirement to inform the DPI or other state institutions about past non-compliance.

ENFORCEMENT

Failure to comply with data processing requirements may potentially raise liability under the Code on Administrative Offenses of the Republic of Lithuania for illegitimate processing of personal data and imply a violation of data subject's

rights. Currently the maximum administrative fine for improper processing of personal data is EUR 289 (EUR 579 for a repeated offense). Peculiarity of the Lithuanian administrative law is that in case of an administrative infringement, the managers of the company is being fined and not the legal entity itself.

The statute of limitation is six months from the offense was identified, in case of continued offenses – within six months after the offense was identified.

Data subjects whose rights have been violated also have the right to claim compensation of damages (economic and moral) in the course of a civil claim. However such type of civil claims in practice are uncommon.

ELECTRONIC MARKETING

Electronic marketing to individuals in Lithuania must only be conducted in accordance with the Data Protection Law, the Electronic Communications Law and the Law on Advertising of the Republic of Lithuania (**Advertising Law**). Only direct marketing tailored to natural persons is subject to the requirements of the above mentioned laws. Direct marketing actions that are targeting legal persons (i.e. companies) are not subject to any of these regulations.

General requirements for direct marketing:

1. The customer has given his prior consent.

   Under Lithuanian law, an opt-in principle applies, i.e. the customer should actively express his willingness to receive commercial communication.

2. The customer consent must be obtained separately from other terms of the contract between the parties.

   Consent cannot be obtained in the standard terms presented to the customer (e.g. “By accepting these terms you agree to receive our commercial communication to the e-mail provided to us”). The consent must stand separately from other contractual terms, so that the data subject has an actual possibility to choose whether he or she wants to receive commercial communication from the company or not.

3. The company must ensure that customers have been given a clear, free-of-charge and easily realisable possibility not to give their consent or refuse giving their consent for the use of this data for the above-mentioned purposes at the time of collection of the data and, if initially the customer has not objected against such use of the data, at the time of each offer.

4. None direct marketing should be carried out where the contact has requested not to receive unsolicited direct marketing.

   Exemption: if the company has obtained a telephone number from its customer within the scope of its business transactions legitimately, the company is permitted to use the telephone number for promotional communication if such communication is regarding similar goods or services of the service provider.

   Additional requirements under the Advertising Law:

1. Direct marketing must be clearly recognisable as commercial communication;

2. The person on behalf of whom this commercial communication is distributed must be clearly identified;

3. The content of the offer and conditions regarding receiving of the service must be formulated clearly and precisely.

Each marketing communication is a separate violation, for which a penalty of up to EUR 580 may be imposed.

ONLINE PRIVACY

Traffic Data. Traffic Data held by a public electronic communications services provider must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

1. it is being used to provide a value added service
2. consent has been given for the retention of the Traffic Data, and
3. it is required for investigation of a grave crime.

Traffic Data can only be processed by a CSP for:

1. the management of business needs, such as billing or traffic
2. dealing with customer enquiries
3. the prevention of fraud, or
4. the provision of a value added service.

Please note that the data retention requirement have not been amended yet as already indicated under section "Law" above.

Cookies. The use of cookies is permitted only if approved by the user (under Lithuanian law, an opt-in principle applies). However, consent is not required for cookies used for website's technical structure and for cookies used for showing website's content. Furthermore, consent is not required for session ID cookies and for so called "shopping basket" cookies (these exceptions do not apply if such cookies are used for collecting statistical information on use of the website).

It is required to provide clear and exhaustive information on use of cookies including information about the purposes of cookies related data processing. This information should be provided in the privacy policy of the website. Consent to the terms of the website's privacy policy or terms of use containing the information on use of cookies is considered insufficient. Consent though web browser settings may be considered adequate only if the browser settings allow choosing what cookies may be used and for what purposes. However, considering the nature of currently used web browsers the consent through web browser settings is not considered appropriate under Lithuanian laws.

Location data. Processing of location data trigger the regulation of personal data processing laws. The data controller must have a legitimate basis for such personal data processing (e.g. the data subject has given his consent; a contract to which the data subject is party is being concluded or performed; it is a legal obligation of the data controller under laws to process personal data; processing is necessary in order to protect vital interests of the data subject; etc.).

KEY CONTACTS

LAWIN
www.lawin.com/

Julius Zaleskis
Senior Associate
T +370 5 2191934
julius.zaleskis@valiunasellex.lt

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

LUXEMBOURG

Last modified 27 January 2016

LAW IN LUXEMBOURG

The law dated 2 August 2002 on the protection of persons with regard to the processing of personal data as amended from time to time ('Law').

The law dated 30 May 2005 laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector as amended from time to time ('Law of 30 May 2005').

DEFINITIONS

Definition of personal data

The Law defines "personal data" as follows: 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); a natural person will be considered to be identifiable if he can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to its physical, physiological, genetic, mental, cultural, social or economic, identity.

Definition of sensitive personal data

Sensitive data relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and health or sex life, including the processing of genetic data.

NATIONAL DATA PROTECTION AUTHORITY

Commission Nationale pour la Protection des Données (CNPD)

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette
T +352 26 10 60 1
F +352 26 10 60 29

The CNPD is in charge of monitoring and checking that processed data are processed in accordance with the provisions of the Law and the Law of 30 May 2005 and their implementing regulations.

REGISTRATION

Prior notification to the CNPD

The processing of personal data, which is not exempt from notification and which is not subject to prior authorisation, must be notified to the CNPD in advance. The notification must contain the information referred to in Article 13 of the Law.

The notifications are performed by completing and signing the notification form provided by the CNPD. Article 12 of the Law provides five general cases and 14 specific cases of exemptions from the obligation to notify:

General exemptions

- processing carried out by the controller if that person appoints a data protection officer (DPO) except for processing for supervision purposes
- processing operations for the sole purpose of keeping a public register
- processing operations carried out by lawyers, notaries and process servers
- processing carried out solely by journalists, or for artistic or literary expression, or
- processing 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 consent.

Conditional exemptions

- processing of data relating exclusively to personal data necessary for the administration of the salaries of persons in the service of or working for the controller
- processing of data relating exclusively to the management of applications and recruitment and the administration of the staff in the service of or working for the controller, provided that the collected data are not sensitive data (including health) or data intended for assessing the data subject
- processing of data relating exclusively to the controller's bookkeeping provided that this data is used exclusively for such bookkeeping and the processing covers only the persons whose data is necessary for bookkeeping purposes
- processing of data referring exclusively to the administration of shareholders, debenture holders and partners, provided that the processing covers solely the data necessary for such administration, the data covers only those persons whose data are necessary for such administration
- processing of data relating exclusively to the management of the controller's client or supplier base, provided that the processed data is not sensitive data (including health)
- processing of data carried out by a foundation, an association or any other non profit organisation
- processing of data relating exclusively to the recording of visitors carried out in the context of manual access control, provided that the data processed is restricted to only the name and business address of the visitor, his/her employer, his/her vehicle, the name, department and function of the person visited, and the time and date of the visit
- processing of identification data essential for communication, which is carried out with the sole purpose of contacting the person concerned provided that these data are not communicated to any other third party
- processing of data carried out by educational establishments with a view to managing their relations with their pupils or students
- processing of data of a personal nature carried out by administrative authorities if the processing is subject to

specific regulations

- processing for the management of computerised and electronic communications systems and networks, provided that it is not used for the purpose of supervision
- processing carried out in hospitals or by a doctor concerning his/her patient, except for the processing of genetic data
- processing carried out by doctors concerning their patients, except for the processing of genetic data, or
- processing carried out by pharmacists other professionals in regulated health professions.

The Law has also reduced the procedures concerning processing in the health professions. Except for the processing of genetic data, there is no requirement of prior authorisation concerning such a processing, and doctors and hospitals are exempt from the obligation to notify.

Prior authorisation by the CNPD

Most processing of personal data must only be notified (unless it is exempt from notification). However, the Law provides for stricter control for processing likely to present specific risks in respect of the rights and freedoms of the individuals concerned. Such processing must be authorised by the CNPD before it may be carried out. Article 14 of the Law sets out the list of these categories of processing.

The prior authorisation by the CNPD is required for:

- the processing of genetic data
- the processing operations for supervision purposes if the data resulting from the supervision are recorded
- data processing for historical, statistical or scientific purposes
- the combination of data
- processing relating to the credit status and solvency of the data subjects, if the processing is carried out by persons other than professionals of the financial sector or insurance companies regarding their clients
- processing involving biometric data necessary for checking personal identity, or
- the usage of data for purposes other than those for which they were collected. Such processing may be carried out only when prior consent has been given by the data subject or if it is necessary to protect the vital interests of the data subject.

Processing operations that reveal race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life and the processing of genetic data are forbidden. However, such prohibition does not apply where:

- the data subject gave his 'express' consent to such processing
- the processing is necessary for the purposes of carrying out the obligations and specific rights of the controller (…) in the field of employment law in so far as it is authorised by law
- 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 consent
- the processing is carried out with the consent of the data subject by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade union aim

- the processing relates to data that have been clearly made public by the data subject
- the processing (…) is necessary to acknowledge, exercise or defend a legal right at law (…)
- the processing is necessary in the public interest for historical, statistical or scientific reasons without prejudice to the conditions for the processing of specific categories of data by the health authorities
- the processing is necessary in the public interest for historical, statistical or scientific reasons or the processing is implemented via a Luxembourg regulation, or
- the processing is implemented in the context of the processing of legal data.

Genetic data may only be processed when the processing is necessary to protect the vital interests of the data subjects or when it is necessary for the purpose of preventive medicine, medical diagnostics, or the provision of care or treatment.

An authorisation from the CNPD is normally required before using technical means for monitoring people, particularly by video camera, electronic tracing, etc. However, the Law has introduced a distinction depending on whether the data are recorded or not.

The prior authorisation by the CNPD is required for processing for supervision purposes, if the data resulting from the supervision are recorded. A simple notification is required if the data resulting from the supervision are not recorded.

For the processing of data relating to credit status and solvency of the data subject, a simple notification is required if the processing is carried out by professionals of the financial sector or insurance companies on behalf of their clients.

The processing of biometric data is subject to prior authorisation.

DATA PROTECTION OFFICERS

The controller may designate a DPO. Such designation releases the controller from the obligation to carry out the notification process. It does not exempt the controller from applying for authorisation before carrying out processing for which authorisation is required.

The powers of the data protection officer are as follows:

- investigative powers to ensure supervision of the controller's compliance with the provisions of the Law and its implementing regulations, and
- a right to be informed by the controller and the relating right to inform the controller of the formalities to be carried out in order to comply with the provisions of the Law and its implementing regulations.

COLLECTION & PROCESSING

Chapter 2 of the Law deals with the conditions under which processing may take place. The controller must ensure that he processes the data in a fair and lawful manner, which means that:

- data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way that is incompatible with those purposes
- the collection, recording and use of personal data is strictly limited to what is necessary to achieve the aims specifically declared in advance by the authority, agency, company, association, professional or self employed worker involved

- processing must be adequate and not excessive in relation to the purposes for which they are collected and/or further processed
- the processing of personal data is limited to cases where there is a direct connection with the initial purpose of the processing. The information must not only be useful, but also necessary to whoever is processing personal data. The data being processed must not be excessive in relation to the aim pursued
- an update of the collected data must be made
- as inaccurate or incomplete information can harm the person to whom it relates, every effort must be made to ensure the data being processed are correct and up to date. If this is not the case, the personal data must be rectified or erased. The Law also protects the data subject against any negative decision automatically made about him by a computer, without him being able to provide his personal point of view, and
- data which permits identification of data subjects are only kept for the necessary period of time.

Legitimacy of processing

The processing of personal data is allowed only if there is a legitimate reason to justify it. According to article 5 of the Law, data may be processed only:

- if it is necessary for compliance with a legal obligation which the controller is subject to
- if it is necessary for the performance of a task carried out in the public interest or in the exercise of public authority
- if it is necessary for the performance of a contract to which the data subject is a party
- if it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and/or freedoms of the data subject
- in order to protect the vital interests of the data subject, or
- if the data subject has given his consent.

Processing of specific categories of data

Processing operations that reveal racial or ethnic origin, politic opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life, including the processing of genetic data, are forbidden and may only be allowed under very exceptional circumstances as listed above. Processing of specific categories of data by the health services is strictly regulated. Legal data and freedom of expression are also strictly regulated.

Processing for supervision purposes

Article 10 of the Law sets out the conditions under which processing for supervision purposes in any place accessible or inaccessible to the public can be made. Processing for supervision purposes is considered legitimate in and around any place presenting a risk where it is necessary not only for the safety of users and the prevention of accidents, but also for the protection of property if there is a serious risk of theft or vandalism. The criteria of necessity and proportionality will be assessed ineach individual case by the CNPD.

The data may only be processed for supervision purposes:

- if the data subject has given his consent

- in surroundings or in any place accessible or inaccessible to the public other than residential premises, particularly indoor car parks, stations, airports and on public transport, provided the place in question due to its nature, position, configuration or frequentation presents a risk that makes the processing necessary for the safety of users and for the prevention of accidents, for the protection of property, if there is a serious risk of theft or vandalism, or

- in private places where the resident natural or legal person is the controller.

The data collected for supervision purposes may be communicated only:

- if the data subject has given his consent, except where forbidden by law

- to the public authorities within the framework of regulations to be enacted pursuant to article 17 (1) of the Law in connection with criminal offences, State security, defence and public safety, criminal law and video surveillance systems for security areas, or

- to the competent legal authorities to record a criminal offence or take legal action in respect of it and to the legal authorities before which a legal right is being exercised or defended'.

Processing for the purposes of supervision at the workplace

The supervision at the workplace is only possible under certain circumstances. Article 11 of the Law refers to Article L.261-1 of the Employment Code. Such processing may be carried out only if it is necessary:

- for the safety and health of employees

- to protect the company's property

- to control the production process relating solely to machinery

- temporarily control production or the employee's services if such a measure is the only way of determining the exact remuneration, or

- in connection with the organisation of work under a flexible schedule in accordance with the Employment Code.

The person whose data are processed must be informed prior to processing. The data subject's consent to the processing does not, however, render the processing legitimate.

TRANSFER

Data may be transferred to a third country, if this country ensures an adequate level of protection and if the provisions of the Law as well as its implementing regulations are complied with.* The adequacy of the level of protection afforded by a third country must be assessed by the controller in light of all circumstances surrounding a data transfer operation or set of data transfer operations; particularly, the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with by that country. In case of any doubt, the controller will immediately inform the CNPD which will consider whether the third country offers an adequate level of protection.

The transfer of data to a third country that does not offer an adequate level of protection may, however, take place, provided:

- the data subject has given his consent to the proposed transfer

- the transfer is necessary for the performance of a contract to which the data subject and the controller are parties, or the implementation of pre-contractual measures taken at the data subject's request
- transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of a legal claim
- the transfer is necessary in order to protect the vital interests of the data subject, or
- the transfer occurs from a public register.

The CNPD may authorise, as a result of a duly reasoned request, a transfer or sets of transfers of data to a third country that does not provide an adequate level of protection, if the controller offers sufficient guarantees in respect of the protection of the privacy, freedoms and fundamental rights of the data subjects, as well as the exercise of the corresponding rights. These guarantees may result from appropriate contractual clauses.

Following the Judgment of the Court of Justice of the European Union on 6 October 2015 (C-362/14) the US-EU Safe Harbor regime is no longer regarded as a valid basis for transferring personal data to the US. In November 2015, the CNPD informed in writing all Luxembourg undertakings who transferred personal data to the US that such transfers made on the basis of the Safe Harbor regime were not legal anymore but were still possible on the basis of appropriate contractual clauses (model clauses) and binding corporate rules

SECURITY

The controller must implement all appropriate technical and organisational measures to ensure the protection of the data he processes against accidental or unlawful destruction or accidental loss, falsification, unauthorised dissemination or access in particularly where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

A description of these measures and of any subsequent major change must be communicated to the CNPD at its request, within fifteen days'.

If the processing is carried out on behalf of the controller, the latter must choose a processor that provides sufficient guarantees as regards the technical and organisational security measures pertaining to the processing to be carried out. Any processing carried out on another person's behalf must be governed by a written contract binding the processor to the controller and providing in particular that the processor will act only on instructions from the controller and the obligations relating to security of processing operations will be also incumbent on the processor.

BREACH NOTIFICATION

Breach notification

Any party that does not carry out the obligation to notify or supplies incomplete or inaccurate information is liable to a fine of between EUR 251 and EUR 125,000.

Breach authorisation

Any party who carries out processing without obtaining the prior authorisation required is liable to a term of imprisonment between eight days and one year and a fine of between EUR 251 and EUR 125,000 or one of these penalties.

ENFORCEMENT

Without prejudice to criminal sanctions provided for by the Law and any actions for damages under civil law, the State

Prosecutor, the CNPD or any injured party may file an action for the immediate cessation of any processing operation made in violation of the legal requirements regarding notification and authorisation, and the temporary suspension of of the activity of the controller or processor.

ELECTRONIC MARKETING

The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing is permissible only in respect of subscribers who have given their prior consent.

Where a supplier obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, that supplier may use those electronic contact details for direct marketing of its own similar products or services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

The transmission of unsolicited communications for purposes of direct marketing by means other than those referred to in the previous paragraphs shall be permissible only with the prior consent of the subscriber concerned.

ONLINE PRIVACY

Traffic Data

For the purposes of the investigation, detection and prosecution of criminal offences, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing traffic data must retain such data for a period of six months. This obligation includes data related to the missed phone calls wherever these data are generated, stored or recorded. Beyond this period, the service provider or operator must erase these data unless they have been made anonymous.

Traffic data may be processed for the purposes of marketing electronic communications services or providing value added services, to the extent and for the duration necessary for such supply or marketing of such services, provided that the provider of an electronic communications service or the operator has informed the subscriber or user concerned in advance of the types of traffic data processed and of the purpose and duration of the processing, and provided that the subscriber or user has given his/her consent, notwithstanding his/her right to object to such processing at any time.

Location Data other than Traffic Data

Service providers or operators have also the obligation to retain location data other than traffic data for a period of six months for the purposes of the investigation, detection and prosecution of criminal offences. This obligation includes data related to missed phone calls wherever these data are generated, stored or recorded. Beyond this period, the service provider or operator must erase these data unless they have been made anonymous.

Service providers or operators may process location data other than traffic data relating to subscribers and users only if such data have been made anonymous or the subscriber or user concerned has given his/her consent thereto, to the extent and for the duration necessary for the supply of a value added service.

Service providers and, where appropriate, operators shall inform subscribers or users in advance of the types of location data other than traffic data processed, of the purposes and duration of the processing and whether the data will be transmitted to third parties for the purpose of providing the value added service. Subscribers or users shall be given the possibility to withdraw their consent to the processing of location data other than traffic data at any time.

Where consent of the subscribers or users has been obtained for the processing of location data other than traffic data, the subscriber or user must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Cookies

Prior informed consent of a subscriber/user is required. The method of providing information and the right to refuse should be as user friendly as possible and, where it is technically possible and effective, the users consent may be expressed by appropriate browser/ application settings.

KEY CONTACTS

Prof. Patrick Van Eecke
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +32 2 500 1630
patrick.van.eecke@dlapiper.com

Eugene H.C. Tchen
Of Counsel
T +352 26 29 04 25 69
eugene.tchen@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MACAU

Last modified 28 January 2015

LAW IN MACAU

Macau personal data protection Law no. 8/2005 of August 22nd ('Law).

DEFINITIONS

Definition of personal data

The Law defines 'personal data' as any information of any type, in any format, including sound and image, related to

- a specific or identifiable natural person ('data subject')
- an identifiable person is anyone who can be identified, directly or indirectly, in particular by reference to a specific number or to one or more specific elements related to his/her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Pursuant to the Law, 'sensitive personal data' can be defined as any personal data revealing political persuasion or philosophical beliefs, political and joint trade unions affiliation, religion, private life and racial or ethnical origin as well as data related to health or sex life, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

'*Gabinete para a Protecção de Dados Pessoais*', in Portuguese, '', in Chinese, and 'Office for Personal Data Protection', in English ('OPDP') is the Macau regulatory authority responsible, inter alia, for supervising and coordinating the implementation of the Law.

Avenida da Praia Grande, n.º 804, Edifício "China Plaza", 13.º andar, A-F, Macau
T: +853 2871 6006
F: +853 2871 6116

www.gpdp.gov.mo

REGISTRATION

The processing of personal data shall be notified to the OPDP by the data processor unless an exemption applies.

For certain data categories (e.g. some sensitive data, data regarding illicit activities or criminal and administrative offences or credit and solvability data) and certain specific personal data processing, prior authorisation from the OPDP is required.

Any variations or changes to the personal data processing determine the amendment of the initial registration.

As for filing requirements, the OPDP provides (official) forms that must be submitted either in Portuguese or Chinese language along with, in particular, the following information (if applicable):

1. identification and contact details of the data processor as well as its representatives
2. the personal data processing purpose
3. identification and contact details of any third party carrying out the personal data processing
4. the commencement date of the personal data processing
5. the categories of personal data processed (disclosing whether sensitive data is to be collected as well as data concerning the suspicion of illicit activities, criminal and/or administrative offences, as well as data regarding credit and solvability)
6. the legitimacy grounds to process personal data
7. the means and forms available to the data subject for updating his/her personal data
8. any transfer of personal data outside Macau, along with the grounds of and measures to be adopted with the transfer
9. personal data storage time limit
10. interconnection of personal data with third parties, and
11. security measures adopted for the protection of personal data.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a data protection officer in Macau.

COLLECTION & PROCESSING

Personal data may only be processed if the data subject has given his/her unequivocal consent or if processing is deemed necessary to:

1. the execution of an agreement where the data subject is a party to or in previous diligences for the conclusion of an agreement at the request of the data subject
2. the compliance of a legal obligation to which the data processor is subject
3. the protection of vital interests of the data subject if he/she is physically or legally unable of giving his/her consent
4. the performance of a public interest assignment or in the exercise of public authority powers vested in the data processor or in a third party to whom the personal data is disclosed, or
5. pursuing a data processor (or a third party to whom the data is disclosed) legitimated interest, provided that the data subject interests or rights, liberties and guarantees shall not prevail.

Moreover, the data subject shall be provided with all relevant processing information, including the identification of the

data processor, the personal data processing purpose and the means and forms available to the data subject for accessing, amending and deleting his/her personal data.

TRANSFER

The transfer of personal data outside Macau can only take place if the recipient country ensures an adequate level of personal data protection.

Exceptionally, the transfer of personal data outside Macau pursuant to a data subject unequivocal consent is allowed. In such case, the data transfer can be carried out immediately after filing the registration with the OPDP.

SECURITY

The data processor must implement adequate technical and organisational measures to protect the personal data against accidental or illicit destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other illicit forms of processing. Such measures shall ensure a security level appropriate to the risks represented by the personal data processing and the nature of the personal data, taking into consideration the state of the art and related costs with its implementation.

BREACH NOTIFICATION

Under the Law, there is no mandatory requirement for data processors to notify the OPDP or data subjects about any personal data breach in Macau.

ENFORCEMENT

Breaches of the Law are subject to civil liability, administrative and criminal sanctions, including fines and/or imprisonment.

ELECTRONIC MARKETING

Under the Law, data subjects have the right to object, on their request and free of charge, to the processing of their personal data for the purpose of direct marketing and to be informed before their personal data is disclosed or used by third parties for the purpose of direct marketing, and to be expressly offered, also free of charge, the right to object to such a disclosure or use.

ONLINE PRIVACY

The rules stated in the Law also apply in the online environment.

For example, where a Macau company collects personal data from Macau residents through its website (by cookies, for instance), such Macau company must fulfil all obligations under the Law imposed on data processors, in particular to inform data subjects of the personal data processing purpose and to duly notify the OPDP about the personal data processing, etc.

KEY CONTACTS

LVT Lawyers
www.lvt-lawyers.com

Tang Weng Hang
Partner
T +853 2871 5588
tangwenghang@lvt-lawyers.com

António Lobo Vilela
Partner
T +853 2871 5588
lobovilela@lvt-lawyers.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MACEDONIA

Last modified 24 March 2015

LAW IN MACEDONIA

In Macedonia, the Law on Personal Data Protection ('Official Gazette of the Republic of Macedonia', nos. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011 and 43/2014) ('DP Law') governs personal data protection issues. The DP Law is entirely harmonized with EC Directive 95/46/EC ('Data Protection Directive'). It entered into force on 8 February 2005 and its current version (following its amendments) is in force as of 11 March 2014.

DEFINITIONS

Defenition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural entity, where an identifiable entity is an entity whose identity can be especially determined, directly or indirectly, on the basis of his/her personal identification number or on one or a combination of features that are specific for his/her physical, mental, economic, cultural or social identity.

Defenition of sensitive personal data

Under the DP Law, sensitive personal data is personal data related to:

- the racial or ethnic origin
- the political views, religious or other beliefs
- membership in a trade union, and
- data relating to the health condition of natural entities, including genetic data, biometric data or data referring to the sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Macedonian data protection authority is the Directorate for Personal Data Protection ('DPA'). It was established in 2005 as an independent state agency with competence to oversee the implementation of the DP Law. The DPA's registered seat is in

Bulevar Goce Delcev 8
Skopje
www.dlzp.mk

REGISTRATION

Any natural or legal entity which intends to collect, process and/or maintain a database containing personal data ('Database') in Macedonia is required to notify the DPA prior to the commencement of any such activity. Exceptionally,

entities which:

- employ less than 10 employees
- intend to process publicly available personal data, or
- intend to process personal data of members of non-profit organisations that are established for political, philosophical, religious or trade-union purposes, are excluded from the notification requirements.

The notification requirements mean that entities are required to register both themselves as data controllers and the respective Databases with so-called Central Register of Databases - an electronic register of data controllers and Databases maintained and managed by the DPA. The registration process is carried out on-line by using the DPA's web application at www.dzlp.mk. A data controller is required to provide all relevant information on particular data processing activities and on its role regarding the same such as: corporate details, purpose of the processing, time period for the retention of processed data, types of the respective data, legal ground for the Database's establishment, transfer of personal data to other countries, security measures for protection of the respective data's integrity, etc.

Following the successful registration, the DPA issues a letter to a data controller by which it confirms that the data controller has fulfilled the notification requirements under the DP Law. Any subsequent changes of the details in the registered Databases have to be reported to the DPA within thirty (30) days from the date when such changes took place.

DATA PROTECTION OFFICERS

The DP Law requires data controllers (only those that are subject to the notification requirements set out in the section 'Registration' above) to appoint a data protection officer. The data protection officer has an overall responsibility to ensure compliance of the data controller with the DP Law and subordinate regulations, in particular the following:

- to participate in the adoption of all decisions relating to the processing of personal data, as well as the exercise of the rights of the data subjects over their personal data
- to draw up the corporate by-laws for personal data protection, including documents relating to the technical and organizational measures for ensuring confidentiality and protection of personal data
- to monitor the compliance of the data controller with the DP Law and other related regulations, especially in relation to the corporate by-laws for protection of the personal data
- to coordinate the internal procedures and guidelines for the personal data protection, and
- ro prepare and deliver a training to the data controller's employees regarding the personal data protection.

COLLECTION & PROCESSING

The DP Law sets out the main principles for the collection and processing of personal data, which require data controllers to collect and process personal data:

- fairly and lawfully
- for legitimate purposes
- proportionally to the needs for the collection and processing,
- accurately and completely, and
- to ensure that the data is stored in a way which enables the identification of the data subjects.

Data controllers are required to obtain a data subject's explicit consent for the collection and processing of his/her personal data (including his/her personal identification number and sensitive personal data). This has to be so-called informed consent which means that data controllers have to provide data subjects with all the relevant details about the particular collection and processing of their personal data (such as the processing's purpose, the data subjects' rights

with respect to the same, retention policy, further transfers, etc). Exceptionally, the DP Law allows data controllers to collect and process personal data without a data subject's consent (eg for the protection of the life or vital interests of the data subjects, protection of the public interest or the exercise of the data controllers' legitimate rights (unless this would jeopardize the fundamental rights and freedoms of the data subjects)).

TRANSFER

Transfer of personal data out of Macedonia is allowed only if the third country in question provides an adequate level of personal data protection. The authority to assess whether a third country provides an adequate level of protection and to approve transfers of personal data out of Macedonia is vested with the DPA. However, an assessment and a subsequent approval from the DPA is not required for a transfer of personal data to the countries which are either:

- members of the European Union ('EU') or the European Economic Area ('EEA'), or
- are 'white-listed'[1] (were assessed to provide an adequate level of the personal data protection) by the European Commission.

The legal assumption that the EU/EEA and 'white-listed' countries provide an adequate level of the personal data protection is enshrined in the DP Law. Moreover, the DP Law completely relies on the European Commission's assessment of the adequacy of a level of protection in non-EU/EEA countries. Therefore, if any third country is assessed by the EC as a country that does not provide an adequate level of legal protection, the transfer of personal data from Macedonia to such country would not be allowed.

In the above context, a transfer of personal data to a country which is not a member of the EU/EEA or a 'white-listed' country is subject to an assessment and approval by the DPA. There is very little practice regarding the approach of the DPA in the process of the respective assessment and approval, nevertheless it is envisaged by the DP Law that the DPA assesses the personal data protection's adequacy in a third country by especially taking into account:

- the nature of the data
- the purpose and duration of the proposed processing
- governing law in the country where the data is to be transferred, and
- protective measures existing in the respective country.

1: Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and the US (only companies that are compliant with the Department of Commerce's Safe Harbour Privacy Principles).

SECURITY

The DP Law does not require data controllers and processors to implement security measures for the protection of personal data by using a particular technology. However, it does require data controllers and processors to undertake appropriate technical and organizational measures for the protection from accidental or illegal damaging of the personal data, or its accidental loss, change, unauthorized disclosing or access, especially when the processing includes a transmission of the data over a network, and for the protection from any kind of illegal processing.

The implemented technical and organisational measures should be proportional to the risk of the data integrity's breach during the processing and the nature of the data being processed. In this context, the DP Law provides guidance for establishing of three levels of personal data protection by using a combination of technical and organizational measures:

1. basic
2. medium
3. high

Both data controllers and processors are required to adopt internal regulations (ie corporate by-laws) containing a description of the technical and organizational measures for the protection of personal data.

BREACH NOTIFICATION

The DP Law does not require data controllers and processors to report data security breaches to the DPA. Accordingly, the DPA is able to trace data security breaches only if a data subject reports a breach of his/her rights or by performing random inspection of data controllers and processors.

ENFORCEMENT

The DPA has an exclusive duty to oversee the implementation and to enforce the DP Law. It has the authority to monitor data controllers and processors' compliance with the DP Law by carrying out random inspections or upon receiving a complaint from a data subject.

If the DPA finds that a data controller and/or processor is in breach of the DP Law, depending on the seriousness of the offence, it may order the remedy of the irregularities within a certain period of time or impose a fine. The fines range from EUR 1,000 to EUR 2,000 (per irregularity) for a legal entity and from EUR 350 to EUR 650 for the responsible person at the legal entity. The DPA is also authorized to request from the data controller and/or processor which breached the DP Law to attend a mandatory training on data protection issues organized by the DPA itself. The only available legal remedy against DPA's decisions for imposing fines on data controllers and/or processors is to initiate an administrative dispute proceeding before the Administrative Court.

Moreover, the Macedonian Criminal Code foresees criminal liability for the misuse of personal data. This criminal offence is punishable with a monetary fine (as determined by the court) or imprisonment for up to one (1) year.

ELECTRONIC MARKETING

The DP Law allows the processing of personal data for the purposes of electronic marketing only if the data subject has explicitly consented to the respective processing provided that the data subject is entitled to withdraw his/her consent at any time free of charge.

ONLINE PRIVACY

There are no specific regulations governing on-line privacy (including cookies). Accordingly, the general data protection rules prescribed by the DP Law apply, to the extent possible, to on-line privacy as well.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Leonid Ristev
Senior Associate
T office +389 2 3223 870, direct +389 2 3223 707
leonid.ristev@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MADAGASCAR

Last modified 25 January 2016

LAW IN MADAGASCAR

Law No. 2014-038 relating to protection of personal data is the main regulatory framework in Madagascar (the 'Data Protection Law').

After discussion at the National Assembly of Madagascar, the Data Protection Law was adopted on 16 December 2014. The Law was promulgated by the President of Republic of Madagascar on 9 January 2015.

In order to come into effect, the Data Protection Law must be published in the Official Gazette of the Republic of Madagascar. This is expected to occur during the course of this year.

DEFINITIONS

Definition of personal data

Personal data is any information relating to a natural person, whereby that person is or can be identified, directly or indirectly, by reference to a name, an identification number or to one or more elements specific to him/her such relating to physical, physiological, psychical, economic, cultural or social.

Definition of sensitive personal data

Sensitive personal data means data which includes information relating to:

- racial origin
- biometric and genetic information
- political opinion
- religious belief or others convictions
- trade-union affiliation
- health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Law provides for the creation of the C*ommission Malagasy sur l'Informatique et des Libertés* ('CMIL'). However, the CMIL has not yet been established.

REGISTRATION

Except for certain data processing that is subject to exemption, authorisation, ministerial order or decree, the processing of personal data requires a prior declaration to the CMIL.

The prior declaration to the CMIL shall specify, where relevant, inter alia:

- the identity and the address of the data controller (*responsable du traitement*) (ie the natural or legal person who either alone or jointly with other persons determines the purpose and the means of the personal data processing and implements such processing itself or appoints a data processor for that purpose)
- the purpose(s) of the processing
- the interconnections between databases
- the types of personal data processed, their origins and the categories of persons affected by the processing
- the duration for which the data will be kept
- the department or persons in charge of implementing the data processing
- the existence of data transfer to other country
- the measures taken in order to ensure the security of the processing
- the use of a data processor (*sous-traitant*).

The CMIL has to issue its decision on any authorisation application 2 months following receipt of the application. An additional time period of 2 months can be added to this period after decision of the President of the CMIL. The absence of decision of the CMIL during these periods is considered as a refusal of the application.

DATA PROTECTION OFFICERS

The Data Protection Law does not provide any legal requirement to appoint a data protection officer (*délégué à la protection des données à caractère personnel)* in Madagascar.

However, an entity is exempt from making prior *declarations* to the CMIL if the entity has appointed a data protection officer ('DPO').

The appointment of a DPO does not exempt an entity from requesting prior *authorisation*, where necessary (for example where there is a transfer of data to a country that does not provide an adequate level of protection for personal data).

The DPO must be a resident of Madagascar.

COLLECTION & PROCESSING

The following principles must be satisfied when personal data is collected and processed:

- all personal data must be processed fairly and lawfully for specific, explicit and legitimate purposes and subsequently processed in accordance with these purposes
- all personal data collected must be adequate, relevant and non-excessive in view of the purposes for which it is collected
- all personal data must be accurate and comprehensive and when necessary, kept up to date
- all personal data must be retained no longer than is necessary for the purposes for which it is processed.

The processing of personal data must receive the data subject's prior consent or fulfill one of the following conditions:

- compliance with a legal obligation of the data controller
- the purpose of the processing is to protect the individual's life

- the purpose of the processing is to carry out a public service
- the processing relates to the performance of a contract to which the concerned individual is a party, or pre-contractual measures requested by that individual
- processing relates to the realisation of the legitimate interest of the data controller or the data recipient, subject to the interest and fundamental rights and liberties of the concerned individual.

The conditions for processing of sensitive personal data include most of the above conditions, but contain an additional list of more restrictive conditions that must also be satisfied such as requirement to obtain prior consent of the data subject, or in the absence of consent where the processing is undertaken to carry out a public service and is required by law or priorly authorised by the CMIL.

TRANSFER

The transfer of a data subject's personal data to a third party country is allowed only if the country guarantees to individuals a sufficient level of protection in terms of privacy and fundamental rights and liberties.

The sufficiency of the protection is assessed by considering all the circumstances surrounding the transfer, in particular the nature of the data, the purpose and the duration of the proposed processing, country of origin and country of final destination, rules of law, both general and sectorial in force in the country in question and any relevant codes of conduct or other rules and security measures which are complied with in that country.

Data controllers may transfer personal data to a third country that is not deemed to offer adequate protection only if:

- the data subject consents and duly informed of the absence of adequate protection
- the transfer is necessary:
    - for the performance of a contract between the data controller and the individual, or pre-contractual measures undertaken at the individual's request
    - for the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party
    - for the protection of the public interest
    - for consultation of a public register intended for the public's information
    - to comply with obligations allowing the acknowledgment, the exercise or the defence of a legal right.

In all cases, the data recipient in the third party country cannot transfer personal data to another country, except with the authorisation of the first data controller and the CMIL .

SECURITY

The data controller must take all useful precautions, with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, amongst other things, prevent alteration, corruption or access by unauthorised third parties.

BREACH NOTIFICATION

The Data Protection Law does not set out any general or specific obligation to notify the CMIL or the data subject in the event of a data security breach.

ENFORCEMENT

The CMIL has the power to proceed with verifications of any data processing, and, as the case may be, to request a copy of every document that it considers useful in respect of verifications. The CMIL agents are authorised to carry out online inspections and on-site verifications of a data controller or a data processor.

In cases where the CMIL is of the opinion that a data controller or a data processor has contravened the provisions of the Data Protection Law, then it may serve, in accordance with the severity of the violation committed:

- warnings and notices to comply with the obligations defined in the Data Protection Law
- notice of withdrawal of the authorisation
- a financial sanction of up to 5% of the last financial year pre-tax turnover (not deducted from tax turnover).

The Data Protection Law provides that any processing of personal data in contravention with its provisions is considered an offence. For example, processing of personal data without prior declaration to or authorisation of the CMIL can result in imprisonment of 6 months to 2 years (Article 62 of the Data Protection Law).

In addition to any penalty, the Court may order the erasure of all or part of the personal data which was the object of the processing considered an offence.

ELECTRONIC MARKETING

The Data Protection Law does not provide specific restrictions on the use of electronic marketing. However, the data subject has a right to opt out of allowing their personal data to be used for marketing purposes without providing any reason.

ONLINE PRIVACY

The Data Protection Law does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Juristconsult Chambers
www.juristconsult.com

Ammar Oozeer
Barrister & Partner
T +(230) 208 5526
aoozeer@juristconsult.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MALAYSIA

Last modified 26 January 2016

LAW IN MALAYSIA

Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 ('PDPA'), was passed by the Malaysian Parliament on 2 June 2010 and came into force on 15 November 2013.

DEFINITIONS

Definition of personal data

'Personal data' means any information in respect of commercial transactions, which:

- is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose
- is recorded with the intention that it should wholly or partly be processed by means of such equipment, or
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Definition of sensitive personal data

'Sensitive personal data' means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister of Information, Communications and Culture ('Minister') may determine by order published in the *Gazette*. Other than the categories of sensitive personal data listed above, the Minister has not '*Gazetted*' any other types of personal data to be sensitive personal data as of 30 November 2015.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to the PDPA, a Personal Data Protection Commissioner ('Commissioner') has been appointed to implement the PDPA's provisions. The Commissioner will be advised by a Personal Data Protection Advisory Committee who will

be appointed by the Minister, and shall consist of one Chairman, three members from the Public sector, and at least seven but no more than eleven other members. The appointment of the Personal Data Protection Advisory Committee shall not exceed a term of three years, however members can be appointed for two terms in succession.

Decisions of the Commissioner can be appealed against through the Personal Data Protection Appeal Tribunal. These are decisions such as:

- decisions relating to the registration of data users under Part II Division 2 of the PDPA
- the refusal of the Commissioner to register a code of practice under Section 23(5) of the PDPA
- the service of an enforcement notice under Section 108 of the PDPA
- the refusal of the Commissioner to vary or cancel an enforcement notice under Section 109, or
- the refusal of the Commissioner to conduct or continue an investigation which is based on a complaint under Part VIII of the PDPA.

If a data user is not satisfied with a decision of the Personal Data Protection Advisory Committee, the data user may proceed to file a judicial review of the decision in the Malaysian High Courts.

REGISTRATION

Currently, the PDPA requires the following classes of data users to register under the PDPA:

1. **Communications**
    1. A licensee under the Communications and Multimedia Act 1998
    2. A licensee under the Postal Services Act 2012
2. **Banking and financial institution**
    1. A licensed bank and licensed investment bank under the Financial Services Act 2013
    2. A licensed Islamic bank and licensed international Islamic bank under the Islamic Financial Services Act 2013
    3. A development financial institution under the Development Financial Institution Act 2002
3. **Insurance**
    1. A licensed insurer under the Financial Services Act 2013
    2. A licensed takaful operator under the Islamic Financial Services Act 2013
    3. A licensed international takaful operator under the Islamic Financial Services Act 2013
4. **Health:**
    1. A licensee under the Private Healthcare Facilities and Services Act 1998
    2. A holder of the certificate of registration of a private medical clinic or a private dental clinic under the Private Healthcare Facilities and Services Act 1998
    3. A body corporate registered under the Registration of Pharmacists Act 1951
5. **Tourism and hospitalities**
    1. A licensed person who carries on or operates a tourism training institution, licensed tour operator, licensed travel agent or licensed tourist guide under the Tourism Industry Act 1992
    2. A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992
6. **Transportation**
    1. Malaysian Airlines System (MAS)
    2. Air Asia
    3. MAS Wings
    4. Air Asia X
    5. Firefly
    6. Berjaya Air
    7. Malindo Air

7. **Education**
    1. A private higher educational institution registered under the Private Higher Educational Institutions Act 1996
    2. A private school or private educational institution registered under the Education Act 1996
8. **Direct selling**
    1. A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993
9. **Services**
    1. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961 carrying on business as follows:
        - legal
        - audit
        - accountancy
        - engineering
        - architecture
    2. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who conducts retail dealing and wholesale dealing as defined under the Control Supplies Act 1961
    3. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who carries on the business of a private employment agency under the Private Employment Agencies Act 1981
10. **Real estate:**
    1. A licensed housing developer under the Housing Development (Control and Licensing) Act 1966
    2. A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah
    3. A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak
11. **Utilities**
    1. Tenaga Nasional Berhad
    2. Sabah Electricity Sdn. Bhd
    3. Sarawak Electricity Supply Corporation
    4. SAJ Holding Sdn. Bhd
    5. Air Kelantan Sdn. Bhd
    6. LAKU Management Sdn. Bhd
    7. Perbadanan Bekalan Air Pulau Pinang Sdn. Bhd
    8. Syarikat Bekalan Air Selangor Sdn. Bhd
    9. Syarikat Air Terengganu Sdn. Bhd
    10. Syarikat Air Melaka Sdn. Bhd
    11. Syarikat Air Negeri Sembilan Sdn. Bhd
    12. Syarikat Air Darul Aman Sdn. Bhd
    13. Pengurusan Air Pahang Berhad
    14. Lembaga Air Perak
    15. Lembaga Air Kuching
    16. Lembaga Air Sibu

Certificates of registration are valid for a period of at least one year (but presently, the Commission grants certificates of registration which are valid for a period of two years), and a data user who fails to renew a certificate of registration and continues to process personal data after the expiry of the certificate of registration commits an offence.

Data users are also required to display their certificate of registration at a conspicuous place at their principle place of business, and a copy of the certificate for each branch, where applicable.

The Commissioner may designate a body as a data user forum in respect of a class of data users. Data user forums can prepare codes of practice to govern compliance with the PDPA which can be registered with the Commissioner.

Once registered, all data users must comply with the provisions of the code, and non-compliance is an offence under the PDPA.

Therefore, companies may want to consider participating in such data user forums to take part in shaping the codes of practice, as this provides them with an opportunity to influence the codes of practice which companies will ultimately have to comply with.

DATA PROTECTION OFFICERS

Currently, there is no requirement for data users to appoint a data protection officer in Malaysia.

COLLECTION & PROCESSING

Under the PDPA, subject to certain exceptions, data users are generally required to obtain the consent of data subjects for the processing (which includes collection and disclosure) of their personal data. Where consent is required from a data subject under the age of eighteen, the data user shall obtain consent from the parent, guardian, or person who has parental responsibility on the data subject.

Further, the consent obtained from a data subject must be in a form that such consent can be recorded and maintained properly by the data user.

There are also other obligations imposed on the data user in relation to the processing of personal data, including, for example, requirements to notify the data subjects regarding the purpose for which their personal data are collected.

In terms of disclosure to third parties, in addition to obtaining the consent of the data subject for such disclosure, data users must ensure that they keep and maintain a list of the disclosures to third parties.

TRANSFER

Under the PDPA, a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister.

However, there are exceptions to this restriction, such as where:

- the data subject has given his consent to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the data user
- the data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner which, if that place were Malaysia, would contravene the PDP, and
- the transfer is necessary to protect the data subject's vital interests.

SECURITY

Under the PDPA, data users have an obligation to take 'practical' steps to protect personal data and in doing so shall develop and implement a security policy. The Commissioner may also from time to time set out security standards which the data user must comply with, and the data user is required to ensure that its data processors also comply with these security standards. No such security standard has been published by the Commissioner as at 30 November 2015.

BREACH NOTIFICATION

There is no requirement under the PDPA for data users to notify authorities regarding data protection breaches in Malaysia.

ENFORCEMENT

Under the PDPA, the Commissioner is empowered to implement and enforce the personal data protection laws and to monitor and supervise compliance with the provisions of the PDPA. Under the Personal Data Protection Regulations 2013, the Commissioner has the power to inspect the personal data system and the data user is required, at all reasonable times, to open the personal data protection system for inspection by the Commissioner or any inspection officer. The Commissioner or the inspection officers may require the production of the following during inspection:

- in relation to general principle, the record of the consent from a data subject maintained in respect of the processing of personal data by the data user
- in relation to notice and choice principle, the record of a written notice issued by the data user to the data subject
- in relation to disclosure principle, the list of disclosure to third parties in respect of personal data that has been or is being processed by him
- in relation to security principle, the security policy developed and implemented by the data user
- in relation to retention principle, the record of compliance in accordance with the retention standard
- in relation to data integrity principle, the record of compliance in accordance with the data integrity standard, and
- such other related information which the Commissioner or any inspection officer deems necessary.

Violation of the PDPA and certain provisions of the Personal Data Protection Regulations 2013 attracts criminal liability. The prescribed penalties include the imposition of fines or a term of imprisonment, or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defence.

However, there is no express right under the PDPA allowing aggrieved data subjects to pursue a civil claim against data users for breaches of the PDPA.

ELECTRONIC MARKETING

The PDPA applies to electronic marketing activities that involve the processing of personal data for the purposes of commercial transactions. There are no specific provisions in the PDPA that deal with electronic marketing. However, the PDPA provides that a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing. 'Direct marketing' means the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

ONLINE PRIVACY

There are no provisions in the PDPA that specifically address the issue of online privacy (including cookies and location data). However, any electronic processing of personal data in Malaysia will be subject to the PDPA and the Commissioner may issue further guidance on this issue in the future.

KEY CONTACTS

Zaid Ibrahim & Co
www.zicolaw.com/

Sharon Tan
Partner
T +603 20879849
sharon.suyin.tan@zicolaw.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MALTA

Last modified 26 January 2016

LAW IN MALTA

The relevant law is the Data Protection Act (Act) (Chapter 440 of the Laws of Malta) and the Regulations (at present nine in number) issued under it.

DEFINITIONS

Definition of personal data

Personal data is defined in the Act as:

'...any information relating to an identified or identifiable natural person; 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 physical, physiological, mental, economic, cultural or social identity'.

Definition of sensitive personal data

Sensitive personal data is also defined in the same Act as meaning:

'...personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life'.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Information and Data Protection Commissioner Airways House

Second Floor
High Street
Sliema SLM 1549
Malta

T +356 2328 7100
F +356 23287198

idpc.info@gov.mt

www.idpc.gov.mt

The Information and Data Protection Commissioner ('Commissioner') has the function (among others) of generally ensuring the correct processing of personal data in order to protect individuals from violations of their privacy.

REGISTRATION

Controllers of data (defined in the Act as persons who alone or jointly with others determine the purposes and means of the processing of personal data), unless exempted by the Commissioner in the circumstances mentioned in the Act or in the circumstances mentioned in Subsidiary Legislation 440.02, must generally notify the Commissioner before carrying out wholly or partially automated processing operations or a set of such operations which are intended to serve either a single or several related purposes. The Commissioner maintains a Register of processing operations which have been notified to him.

The Register must contain the following information:

- the name and address of the data controller and of any other person authorised by him in that respect, if any
- the purpose or purposes of the processing
- a description of the category or categories of data subject and of the data or categories of data relating to them
- the recipients or categories of recipient to whom the data might be disclosed, and
- proposed transfers of data to third countries.

DATA PROTECTION OFFICERS

Under Maltese law there is presently no obligation to appoint data protection officers. However, the Act states that the controller of personal data shall notify the Commissioner on the appointment or removal of a personal data representative (if any). The personal data representative has the function (among others) of independently ensuring that the controller processes personal data in a lawful and correct manner and in accordance with good practice and in the event of the personal data representative identifying any inadequacies, he shall bring these to the attention of the controller.

COLLECTION & PROCESSING

Personal data may be processed (which includes also the collection of data) only if:

- the data subject has unambiguously given his consent
- processing is necessary for the performance of a contract to which the data subject is a party to or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed, or
- processing is necessary for 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.

If the data subject gives notice to the controller of his opposition, personal data cannot be processed for the purposes of direct marketing.

As a general rule, sensitive personal data cannot be processed except in the cases mentioned in the Act (eg where the

data subject has given his explicit consent to processing or has made the data public).

The data subject has a right to be provided, by the controller or any person authorised by him, with information such as the identity and habitual residence, or principal place of business, of the controller and of any other person authorised by him in that respect; the purpose of the processing; and any further information relating to matters such as the recipients of the data, whether the reply to any questions made to the data subject is obligatory or voluntary and the existence of the right to access, rectify and erase the data concerning him. The controller must guarantee fair processing in respect of the data subject.

TRANSFER

The controller must always notify the Commissioner of any proposed transfers of data to third countries, since such transfers also constitute 'processing' under Maltese law. 'Third countries' only include countries which are not Member States of the European Union. The transfer may only take place if the third country to which the data is to be transferred ensures an adequate level of protection. Whether the country ensures such a level of protection shall be decided by the Commissioner.

A transfer of data to a third country that does not ensure an adequate level of protection may still be effected by the controller but only if the data subject gives his unambiguous consent to the proposed transfer or if the transfer:

- is necessary for the performance of a contract between the data subject and the controller or the implementation of pre contractual measures taken in response to the data subject's request
- is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party
- is necessary or legally required on public interest grounds, or for the establishment, exercise or defence of legal claims
- is necessary in order to protect the vital interests of the data subject, or
- is made from a register that according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided that the conditions laid down in law for consultation are fulfilled in the particular case.

In these cases the Commissioner's approval is not generally required but the transfer must still be notified.

The Commissioner has the power to authorise such a transfer of personal data to a third country that does not ensure an adequate level of protection provided however that the controller provides adequate safeguards, such as by contractual provisions, with respect to the protection of privacy and fundamental human rights. The way this seems to be interpreted by the Maltese Office of the Information and Data Protection Commissioner is that despite the grounds listed above (including consent of the data subject), the Commissioner may still require the said adequate safeguards before authorising a transfer to a third country not offering an adequate level of protection. The EU model clauses and/or Binding Corporate Rules (for intra-group transfers) are often invoked by controllers wishing to transfer personal data to such countries. In these cases the Commissioner's approval is not automatic and applicants must file evidence of any additional safeguards that may exist.

The Minister responsible for freedom of information and data protection may also designate by Order, in order to implement any international convention to which Malta is party or any other international obligation of Malta, that the transfer of personal data to any country listed in the Order shall not be restricted on grounds of protection of privacy.

Apart from mere notification to the Commissioner, no other restrictions or formalities apply in relation to transfer of personal data to:

- member States of the European Union;

- member States of the EEA; or
- third countries which are recognised by the EU Commission to have an adequate level of protection.

It should be noted that following the judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbour regime is no longer regarded as a valid basis for transferring personal data to the US. Data Controllers previously relying on the Safe Harbour scheme to transfer personal data from Malta to the USA, are therefore required to use alternative mechanisms (such as data transfer agreements containing 'standard contract clauses') as provided for under national law in order to guarantee an adequate level of data protection for such transfers. *Approval* by the Commissioner for such transfers is now required – as opposed to mere *notification* – in those cases previously relying exclusively on the 'safe harbour' procedure. EU model clauses and/or BCRs (if applicable) may be used in this regard. As discussed above, the Commissioner's approval is not automatic and all relevant evidence of adequate safeguards in place must be filed.

The Maltese Office of the Information and Data Protection Commissioner has recently updated its website to reflect the outcome of the ***Schrems*** judgment. The updated text regarding data transfers can be accessed here:

http://idpc.gov.mt/article.aspx?art=121

SECURITY

Data controllers must implement the appropriate technical and organisational measures to protect personal data which is processed against accidental destruction or loss or unlawful forms of processing. An adequate level of security must be provided which gives regard to:

- the technical possibilities available;
- cost of implementing the security measures;
- special risks that exist in the processing of personal data; and
- sensitivity of the personal data being processed.

If a processor is engaged by the controller, the controller must ensure that the processor can implement the necessary security measures and that the processor actually takes such measures.

BREACH NOTIFICATION

Legal Notice 239 of 2011, which was brought into force as of 1st January 2013, has amended Subsidiary Legislation 440.01, Processing of Personal Data (Electronic Communications Sector) Regulations, making new provisions for breach notifications.

The Regulations provide that, in the case of a personal data breach, the provider of publicly available electronic communications service must notify the breach to the Commissioner without delay. 'Personal data breach' will be defined in the Regulations as *'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service'.*

If the breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider must also notify the subscriber or individual of the breach without delay. However, notification to the subscriber or individual

concerned shall not be required on the condition that the provider demonstrates to the satisfaction of the Commissioner that he has implemented appropriate technological protection measures and that those measures were applied to the data concerned by the security breach. Such technological protection measures should render the data unintelligible to any person who is not authorised to access it.

If the provider has not already notified the subscriber or individual of the personal data breach, the Commissioner may require the provider to do so after considering the likely adverse effects of the breach.

The notification to the subscriber or individual must at least include the nature of the breach and the contact points where more information can be obtained. The notification must also recommend measures to mitigate the possible adverse effects of the breach. The notification to the Commissioner shall also include the consequences of and the measures proposed or taken by the provider to address the breach. The Regulations also provide that the Commissioner is to encourage the drawing up of guidelines and where necessary issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format which such notification is to take and the manner in which the notification is to be made.

Service providers are to maintain an inventory of personal data breaches consisting of the facts surrounding the breach, its effects and the remedial action taken which must be sufficient so as to enable the Commissioner to verify compliance with the provisions of the Regulations.

ENFORCEMENT

The Act states that any person who does not comply with any lawful request relevant to an investigation by the Commissioner shall be guilty of an offence under the Act.

In the exercise of his functions under the Act, the Commissioner has the same powers to enter and search any premises as are vested in the executive police by any law as may be in force from time to time.

If the Information and Data Protection Commissioner concludes that personal data is processed or may be processed in an unlawful manner, the Commissioner shall order rectification, and if rectification is not effected or if the matter is urgent, the Commissioner may prohibit the controller of personal data to continue processing the personal data in any manner other than to store that data.

If the controller does not implement security measures in terms of the Act, or transfers personal data to third countries in contravention of the Act or fails to notify the Data Protection Commissioner in terms of the Act, the Commissioner may impose an administrative fine as prescribed (see below for more information on fines and penalties).

Where the Data Protection Commissioner decides that personal data has been unlawfully processed, the said Commissioner shall by notice order the controller of personal data to erase the personal data.

Any person aggrieved by a decision of the Commissioner shall have the right to appeal in writing to the Information and Data Protection Appeals Tribunal within thirty days from the notification to him of the said decision.
Any party to an appeal to the said Tribunal who feels aggrieved by a decision of the Tribunal, or the Commissioner if he feels aggrieved with any such decision, may on a question of law appeal to the Court of Appeal of Malta within thirty days from the date on which that decision has been notified.
It should be noted that if controllers feel aggrieved by a decision of the Commissioner to order the erasure of personal data, the controller of personal data must (within fifteen days from the receipt of the Commissioner's notice) seek redress, by requesting (by way of application) the Court of Appeal of Malta to revoke the order of the Commissioner.

Fines and Penalties

Recently, the Act has been amended to address two separate frameworks, one for administrative fines that may be imposed by the Commissioner and another for court penalties. A clear distinction between administrative fines and court penalties was introduced by means of a separate definition for each of the two types of sanctions and the Act now establishes a procedure for their imposition. Moreover, schedules to the Act were introduced in order to assist, inter alia,

in identifying which of the offences are liable to administrative fines and which are liable to court penalties. Parameters were also established with regards to the minimum and maximum amount of fines and penalties that may be imposed for each respective breach.

Sanctions under the Act are both civil and criminal. A data controller in breach of the Act may, inter alia, be liable (for each violation/offence) to: (i) an administrative fine imposed by the Commissioner; (ii) an order to pay compensation to the aggrieved data subject following a successful action for damages by the data subject; or (iii) a criminal fine (currently a maximum of EUR23,300) or imprisonment (currently a maximum of six months) or both.

1. The various administrative fines that may be imposed by the Commissioner vary in nature (there are three levels of fines) and must be examined on a case-by-case basis. The maximum fine that may be imposed is of €23,300 for each violation with an additional (maximum) of €2,500 as a daily fine for each day during which the violation in question subsists. Fines of this nature are generally deemed as civil debts in favour of the Commissioner.
2. An aggrieved data subject may, by sworn application filed in the competent Civil Court, exercise an action for damages against a data controller who processes data in contravention of the Act. Such action must be commenced within 12 months from the date when the said data subject becomes aware or could have become aware of such a contravention, whichever is the earlier.
3. The various (criminal) penalties which are enforceable by prosecution in the Courts of Malta also vary depending on the offence in question (here too, there are three levels of penalties). The maximum penalty ('multa') that may be imposed is of €23,300 per violation or a term of imprisonment of not more than six months (per violation) or both such fine and imprisonment (depending on the matter at hand).

ELECTRONIC MARKETING

The Act applies also to most electronic marketing activities since in the course of such activities, it is likely that 'personal data' as defined above (including e-mails) will be 'processed' as understood by the Act. In relation to direct marketing (even electronic), consent may be revoked at will by the data subject(s). The controller is legally bound to inform the data subject that he/she may oppose such processing at no cost.

Apart from the Act, the 'Processing of Personal Data (Electronic Communications Sector) Regulations 2003' (Legal Notice 16 of 2003 as amended) (the 'Electronic Communications Regulations') address a number of activities relating specifically to electronic marketing.

In the case of subscriber directories, the producer of such directories shall ensure (without charge to the subscriber) that before any personal data relating to the subscriber (who must be a natural person) is inserted in the directory, the subscriber is informed about the purposes of such a directory of subscribers and its intended uses (including information regarding search functions embedded in the electronic version of the directories). No personal data shall be included without the consent of the subscriber. In furnishing his consent the subscriber shall determine which data is to be included in the directory and he is free to change, alter or withdraw such data at a later date. The personal data which shall be used in the directory must be limited to what is necessary to identify that subscriber and the number allocated to him, unless the subscriber has given his additional consent authorising the inclusion of additional personal data.

The Electronic Communications Regulations also deal with the issue of unsolicited communications. A person is prohibited from using any publicly available electronic communications service to engage in unsolicited communications for the purpose of direct marketing by means of:

- an automatic calling machine;
- a facsimile machine; or
- electronic mail

to a subscriber, irrespective of whether such subscriber is a natural person or a legal person, unless the subscriber has

given his prior explicit consent in writing to the receipt of such a communication.

By way of exception to the above, where a person has obtained from his customers their contact details for electronic mail in relation to the sale of a product or a service, in accordance with the Act that same person may use such details for direct marketing of its own similar products or services. However, the customers must be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

Allowing the recipient to send a request requesting that such communication cease, is strictly prohibited.

In all cases the practice of inter alia sending electronic mail for the purposes of direct marketing, disguising or concealing the identity of the sender or without providing a valid address to which the recipient may send a request that such communications cease shall be prohbited.

ONLINE PRIVACY

Cookie Compliance

Legal Notice 239 of 2011 entitled 'Processing of Personal Data (Electronic Communications Sector)(Amendment) Regulations 2011 was brought into force with effect as of 1st January 2013. This Legal Notice amended the regulations thereby implementing into Maltese Law the amendments under Article 2(5) of Directive 2009/136/EC. Having said the above, the Maltese Office of the Data Protection Commissioner ('DPC') is still in the process of drafting local guidelines on the way in which the so called 'cookie clause' is to be interpreted. We have no information indicating when these guidelines may be published. It is worth noting that the DPC's website presently makes reference to the Article 29 Data Protection Working Party Document 02/2013 providing guidance on obtaining consent for cookies (adopted on 2 October 2013).

Traffic Data

In terms of the Electronic Communications Regulations, traffic data relating to subscribers and users processed by an undertaking which provides publicly available electronic communications services or which provides a public communications network, shall be erased or made anonymous when it is no longer required for the purpose of transmitting a communication.

Traffic data required for the purposes of subscriber billing or interconnection payments may be retained provided however that the retaining of such data shall only be permissible up to the period during which the bill may be lawfully challenged or payment pursued.

Furthermore, traffic data may be processed where the aim is to market or publicise the provision of a value-added service, however, the processing of such data shall only be permissible to the extent and for the duration necessary to render such services.

Processing of traffic data is also permissible by an undertaking providing publicly available electronic communication for the following purposes:

- managing billing or traffic management;
- customer enquiries;
- fraud detection; and
- rendering of value-added services.

Location Data

Where location data (other than traffic data) relating to users or subscribers of public communications networks or of publicly available electronic communications services can be processed, such data may only be processed when it is made anonymous or with the consent of the users or subscribers, to the extent and for the duration necessary for the

provision a value-added service.

Prior to obtaining the user or subscriber's consent, the undertaking providing the service shall inform them of the following:

- the type of location data which shall be processed
- the purpose and duration of processing, and
- whether the processed data shall be transmitted to a third party for the purpose of providing the value-added service.

A user and/or subscriber may withdraw their consent for the processing of such location data (other than traffic data) at any time.

%MCEPASTEBIN%%MCEPASTEBIN%%MCEPASTEBIN%

KEY CONTACTS

Mamo TCV Advocates
www.mamotcv.com/

Dr. Antoine Camilleri
Partner
T +356 21 231 345
antoine.camilleri@mamotcv.com

Dr. Claude Micallef-Grimaud
Senior Associate
T +356 21 231 345
claude.micallefgrimaud@mamotcv.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MAURITIUS

Last modified 25 January 2016

LAW IN MAURITIUS

The Data Protection Act (the 'Act') was enacted by the National Assembly in 2004 with the aim of protecting the fundamental privacy rights of individuals against the use of data concerning them without their informed consent. The Act came into operation in February 2009.

DEFINITIONS

Definition of personal data

'Personal data' means:

- data which relate to an individual who can be identified from those data
- data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion.

Definition of sensitive personal data

Sensitive personal data is defined under the Act as personal information concerning a data subject and consisting of information pertaining to:

- racial or ethnic origin
- political opinion or adherence
- religious belief or other belief of a similar nature
- membership of a trade union
- physical or mental health
- sexual preferences or practices
- the commission or alleged commission of an offence
- any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Office

5th Floor, Happy World House
Corner SSR and Sir William Newton Streets,
Port Louis, Mauritius

Tel: +230 212 22 18
Fax: +230 212 21 74

http://dataprotection.govmu.org/

REGISTRATION

Every data controller and every data processor must:

- apply for registration in writing to the Data Protection Commissioner
- together with the application, provide certain particulars.

The particulars to be provided by a data controller in its application for registration are the following:

- its name and address, if it has nominated a representative for the purposes of the Act, the name and address of the representative
- a description of the personal data being, or to be processed by or on behalf of the data controller, and of the category of data
- subjects, to which the personal data relates
- a statement as to whether or not he holds, is likely to hold, sensitive personal data
- a description of the purpose for which the personal data is or will be processed
- a description of any recipient to whom the data controller intends or may wish to disclose the personal data
- the names, or a description of, any country to which the data controller directly or indirectly transfers, or intends or may wish, directly or indirectly, to transfer the data
- the class of data subjects, or where practicable the names of data subjects, in respect of whom the data controller holds personal data.

The particulars to be provided by a data processor in its application for registration are the following:

- its name and address
- a description of the personal data being, or to be processed, and the category of data subjects to which the personal data relates
- the country to which it transfers, or intends to transfer, the personal data
- a statement as to whether or not it processes, or intends to process, sensitive personal data
- such other particulars as the Data Protection Commissioner may require.

Where the data controller or data processor intends to keep or process personal data or sensitive personal data for two or more purposes, it must make an application for separate registration in respect of each of those purposes and, entries shall be made in accordance with any such applications. The Data Protection Commissioner shall grant an application for registration, unless he reasonably believes that:

- the particulars proposed for inclusion in an entry in the register are insufficient or any other information required by the Data Protection Commissioner either has not been furnished, or is insufficient
- appropriate safeguards for the protection of the privacy of the data subjects concerned are not being, or will not continue to be, provided by the data controller

- the person applying for registration is not a fit and proper person.

Registration is for a period not exceeding one year and on expiry of such period, the relevant entry shall be cancelled unless the registration is renewed.

A data controller or a data processor who, without reasonable excuse or lawful authority, keeps or processes any personal data or sensitive personal data, without registering himself or renewing his registration, shall commit an offence.

DATA PROTECTION OFFICERS

The Act does not provide any legal requirement to appoint a data protection officer.

COLLECTION & PROCESSING

A data controller must not collect personal data unless:

- it is collected for a lawful purpose connected with the function or activity of the data controller, and
- the collection of the data is necessary for that purpose.

If the data controller collects personal data directly from the data subject, the data controller must at the time of collecting personal data ensure that the data subject concerned is informed of the following:

- the fact that the data is being collected
- the purpose or purposes for which the data is being collected
- the intended recipients of the data
- the name and address of the data controller
- whether or not the supply of the data by that data subject is voluntary or mandatory
- the consequences for that data subject if all or any part of the requested data is not provided
- whether or not the data collected shall be processed and whether or not the consent of the data subject shall be required for such processing, and
- his right of access to, the possibility of correction of and destruction of, the personal data to be provided.

If data is not collected directly from the data subject concerned, the data controller or any person acting on his behalf must ensure that the data subject is informed of the matters set out above.

Generally a data controller cannot process personal data unless it has obtained the express consent of the data subject. However, personal data may nevertheless be processed without obtaining the express consent of the data subject where the processing is necessary:

- for the performance of a contract to which the data subject is a party
- in order to take steps required by the data subject prior to entering into a contract
- in order to protect the vital interests of the data subject
- for compliance with any legal obligation to which the data controller is subject
- for the administration of justice, or

- in the public interest.

Sensitive personal data cannot be processed unless the data subject:

- has given his express consent to the processing of the personal data, or
- made the data public.

The above requirements will not apply to the processing of sensitive personal data if such processing:

- is necessary:
    - in order to protect the vital interests of the data subject or another person in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject
    - in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld
    - for the performance of a contract to which the data subject is a party
    - in order to take steps required by the data subject prior to entering into a contract, or
    - for compliance with a legal obligation to which the data controller is subject
- is required by any investigatory authority under the Financial Intelligence and Anti-Money Laundering Act, or
- is required by law.

TRANSFER

A data controller cannot, except with the written authorisation of the Data Protection Commissioner, transfer personal data to another country.

The Act provides that, personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

However, the adequacy and the level of protection of a country shall be assessed in the light of all the circumstances surrounding the data transfer, having regard in particular to:

- the nature of the data
- the purpose and duration of the proposed processing
- the country of origin and the country of final destination
- the rules of law, both general and sectoral, in force in the country in question, and
- any relevant codes of conduct or other rules and security measures which are complied with in that country.

The above data protection principle shall not apply where:

- the data subject has given his consent to the transfer
- the transfer is necessary:
    - for the performance of a contract between the data subject and the data controller, or for the taking of

steps at the request of the data subject with a view to his entering into a contract with the data controller

- for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered into at the request of the data subject, or is in the interest of the data subject, or for the performance of such a contract, or

- in the public interest, to safeguard public security or national security.

- the transfer is made on such terms as may be approved by the Data Protection Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.

SECURITY

A data controller shall:

- take appropriate security and organisational measures for the prevention of unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of the data in his control, and

- ensure that the measures provide a level of security appropriate to the harm that might result from the unauthorized access to, alteration, disclosure, destruction of the data or its accidental loss, and the nature of the data concerned.

A data controller or a data processor must take all reasonable steps to ensure that any person employed by him is aware of and complies with the relevant security measures.

In determining the appropriate security measures, in particular, where the processing involves the transmission of data over an information and communication network, a data controller must have regard to:

- the state of technological development available
- the cost of implementing any of the security measures
- the special risks that exist in the processing of the data, and
- the nature of the data being processed.

BREACH NOTIFICATION

Breach notification

The MU DPA provides for an option to make a complaint There is no mandatory requirement in the Act to report data security breaches or losses to the Data Protection Commissioner or to data subjects. However, the Act provides that a complaint may be made to the Data Protection Commissioner that the Act or any regulations made under it has been, is being, or is about to be contravened. If a complaint is made, the Data Protection Commissioner shall:

- investigate the complaint or cause it to be investigated by an authorised officer, unless he is of the opinion that such complaint is frivolous or vexatious

- as soon as reasonably practicable, notify the complainant in writing of his decision in relation to the complaint and that the complainant may, if he is aggrieved by the Data Protection Commissioner's decision, appeal to the ICT Appeal Tribunal.

Mandatory breach notification

None contained in the Act.

ENFORCEMENT

The Data Protection Commissioner is responsible for the enforcement of the Act.

If the Data Protection Commissioner is of the opinion that a data controller or a data processor has contravened, is contravening or is about to contravene the Act, the Data Protection Commissioner may serve an enforcement notice on the data controller or the data processor, as the case may be, requiring him to take such steps within such time as may be specified in the notice.

A person who, without reasonable excuse, fails or refuses to comply with an enforcement notice commits an offence, and is, on conviction, liable to fine not exceeding 50,000 rupees (approximately £1,000) and to imprisonment for a term not exceeding 2 years.

The Data Protection Commissioner may apply to a Judge in Chambers for an order for the expeditious preservation of data, including traffic data, where she has reasonable grounds to believe that such data is vulnerable to loss or modification. If the Judge in Chambers is satisfied that such an order may be made, he shall issue a preservation order specifying a period which shall not be more than 90 days during which the order shall remain in force. The Judge in Chambers may, on application made by the Data Protection Commissioner, extend the 90 days period.

If the Data Protection Commissioner is of the opinion that the processing or transfer of data by a data controller or data processor entails specific risks to the privacy rights of data subjects, he may inspect and assess the security measures taken prior to the beginning of the processing or transfer.

The Data Protection Commissioner may, at any reasonable time during working hours, carry out further inspection and assessment of the security measures imposed on a data controller or data processor. The Data Protection Commissioner may carry out periodical audits of the systems of data controllers or data processors to ensure compliance with the data protection principles as set out in the Act.

On completion of an investigation under the Act, the Data Protection Commissioner shall, where the investigation reveals that an offence has been committed under the Act or any regulations made under the Act, refer the matter to the Police.

ELECTRONIC MARKETING

The Act does not prohibit the use of personal data for the purposes of electronic marketing but it provides individuals with the right to prevent the processing of their personal data (e.g. a right to opt out) for direct marketing purposes.

A person may, at any time, by notice in writing, request a data controller to stop or not to begin the processing of personal data in respect of which he is a data subject, for the purposes of direct marketing. Direct marketing is defined as communication of any advertising or marketing material which is directed to any particular individual. When the data controller receives a request from a data subject, he shall, as soon as reasonably practicable and in any event not more than 28 days after the request has been received:

- where the data is kept only for purposes of direct marketing, erase the data, and
- where the data is kept for direct marketing and other purposes, stop processing the data for direct marketing.

The data controller must notify the data subject in writing of any action taken and, where appropriate, inform him of the other purposes for which the personal data is being processed.

ONLINE PRIVACY

The Act does not contain specific provisions in relation to online privacy.

In relation to traffic data, the Act provides that the Data Protection Commissioner may apply to a Judge in Chambers for an order for the expeditious preservation of data, including traffic data, where he has reasonable grounds to believe that such data is vulnerable to loss or modification. Traffic data is defined in the Act as any data relating to a communication by means of a computer system, which is generated by the system and forms part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

KEY CONTACTS

Juristconsult Chambers
www.juristconsult.com

Ammar Oozeer
Barrister & Partner
T +(230) 208 5526
aoozeer@juristconsult.com

Arvin Halkhoree
Barrister
T +(230) 208 5526
ahalkhoree@juristconsult.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MEXICO

Last modified 24 March 2015

LAW IN MEXICO

The Federal Law on the Protection of Personal Data held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) (the 'Law') was enacted on July 5, 2010 and entered into force on July 6, 2010.

The Executive Branch has also issued:

- the Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) on December 21, 2011 (the 'Regulations'), same which entered into force on December 22, 2011
- the Privacy Notice Guidelines on January 17, 2013 (the 'Guidelines') which entered into force on April 18, 2013
- the Parameters for Self Regulation regarding personal data on May 29, 2014 (the 'Parameters'), which entered into force on May 30, 2014

The Regulations apply to all personal data processing when:

- processed in a facility of the data controller located in Mexican territory
- processed by a data processor, regardless of its location, if the processing is performed on behalf of a Mexican data controller
- where the Mexican legislation is applicable as a consequence of Mexico's adherence to an international convention or the execution of a contract (even where the data controller is not located in Mexico), or
- where the data controller is not located in Mexican territory but uses means located in Mexico to process personal data, unless such means are used only for transit purposes.

The Law only applies to private individuals or legal entities which process personal data, and not to the government, credit reporting companies governed by the Law Regulating Credit Reporting Companies, or persons carrying out the collection and storage of personal data exclusively for personal use and without the purposes of disclosure or commercial use.

DEFINITIONS

Definition of personal data

'Personal Data' is any information concerning an identified or identifiable individual.

Definition of sensitive personal data

'Sensitive Personal Data' is all personal data touching on the most intimate areas of the data subject's life, which misuse may lead to discrimination or serious risk to the data subject. In particular, the definition includes data that may reveal:

- racial or ethnic origin
- present or future health conditions
- genetic information
- religious, philosophical or moral beliefs
- union affiliation
- political views, and
- sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

The Federal Institute for Access to Information and Data Protection (*Instituto Federal de Acceso a la Información y Protección de Datos*) (IFAI) and the Ministry of Economy (*Secretaría de Economía)*.

REGISTRATION

Not required.

DATA PROTECTION OFFICERS

All data controllers are required by Law to designate a personal data officer or department (jointly hereinafter referred to as the 'Data Protection Officer') to handle requests from data subjects exercising their rights under the Law. Data Protection Officers are also responsible for enhancing the protection of personal data within their organizations.

COLLECTION & PROCESSING

The term 'processing' is broadly defined to include the collection, use, communication, or storage of personal data by any means. Use includes all access, management, procurement, transfer and disposal of personal data.

In processing personal data, data controllers must observe the principles of legality, consent, notice, quality, purpose, loyalty, proportionality and accountability.

Personal data must be:

- collected and processed fairly and lawfully
- collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes
- adequate, relevant and not excessive in relation to the purposes for which it is collected and/ or further processed
- accurate and, if necessary, updated; every reasonable step must be taken to ensure that data which 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
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data, – ie, reliance on the assumption that the personal data will be processed as agreed upon by the parties (in the privacy notice or

otherwise) and in compliance with the Law.

To legally process personal data, data controllers must provide a privacy notice (*Aviso de Privacidad*) (the 'Privacy Notice'), which must be made available to a data subject prior to the processing of his or her personal data. The Privacy Notice may be provided to data subjects in printed, digital, visual or audio formats, or any other technology.

A comprehensive Privacy Notice must at least contain:

- the identity and domicile of the data controller collecting the data
- the purposes of the data processing
- the options and means offered by the data controller to data subjects to limit the use or disclosure of their data
- the means for exercising rights of access, correction, cancellation or objection (ARCO rights) in accordance with the provisions of the Law
- where appropriate, the types of data transfers to be made
- the procedure and means by which the data controller will notify the data subjects of changes to the Privacy Notice, and
- when processing sensitive personal data, the Privacy Notice must clearly state that sensitive personal data will be processed.

The Guidelines consider three forms of privacy notice: comprehensive, simplified and short form, depending on whether the data is personally obtained from the data subject, the data is obtained directly or indirectly from the data subject, or the space to obtain data is minimal or limited (where the space allotted for the gathering of personal data or the Privacy Notice is also minimal or limited), respectively. Each of these forms must meet specific disclosure requirements.

The data controller has the burden of proof to show that the Privacy Notice was provided to the data subject prior to the processing of his data.

Consent is required for all processing of personal data, except as otherwise provided by the Law. Implicit consent (notice and opt out) applies to the processing of personal data; express consent (notice and opt in) applies to the processing of financial or asset data; and express and written consent applies to the processing of sensitive personal data. Consent may be communicated verbally, in writing, by electronic or optical means, via any other technology, or by any other unmistakable indications. Express written consent may be obtained through the data subject's written signature, electronic signature, or any other authentication mechanism set up for such purpose.

Consent from the data subject will not be required for the processing of personal data when:

- any law so provides
- the data is contained in publicly available sources
- the identity of the data subject has been disassociated from the data
- processing has the purpose of fulfilling obligations under a legal relationship between the data subject and the data controller
- there is an emergency situation that could potentially harm an individual with regard to his person or property
- processing is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data subject is unable to give consent in the manner established by the General Health Law (*Ley General de Salud*) and other applicable laws, and said processing is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or

- pursuant to a resolution issued by a competent authority.

TRANSFER

Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide the third parties with the Privacy Notice and the purposes to which the data subject has limited the data processing.

Data processing will be in accordance with what was agreed in the Privacy Notice, which shall contain a clause indicating whether or not the data subject agrees to the transfer of his data; moreover, the third party recipient will assume the same obligations as the data controller who has transferred the data.

Domestic or international transfers of personal data may be carried out without the consent of the data subject where:

- the transfer is pursuant to a law or treaty to which Mexico is party
- the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management
- the transfer is made to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies
- the transfer is necessary by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject
- 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 a right in a judicial proceeding, or
- where the transfer is necessary to maintain or comply with an obligation resulting from a legal relationship between the data controller and the data subject.

The Regulations establish that communications or transmissions of personal data to data processors need not to be informed nor consented to by the data subject. However, the data processor must:

- process personal data only according to the instructions of the data controller
- not process personal data for a purpose other than as instructed by the data controller
- implement the security measures required by the Law, the Regulations, and other applicable laws and regulations
- maintain confidentiality regarding the personal data subject to processing
- eliminate personal data that were processed after the legal relationship with the data controller is concluded or upon instructions of the data controller, provided there is no legal requirement for the preservation of the personal data, and
- not transfer personal data unless the data controller so determines, the communication arises from subcontracting, or if so required by a competent authority.

The agreement between the data controller and data processor related to the processing of personal data must be in accordance with the corresponding Privacy Notice provided to the data subject.

SECURITY

All data controllers must establish and maintain physical, technical and administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorised use, access or processing. They may not adopt security measures that are inferior to those they have in place to manage their own information.

The risk involved, potential consequences for the data subjects, sensitivity of the data, and technological development must be taken into account when establish security measures.

BREACH NOTIFICATION

Security breaches occurring at any stage of the processing which materially affect the property or moral rights of the data subject must be promptly reported by the data controller to the data subject, so that he can take appropriate action to defend his rights.

The Regulations provide that breach notification must include at least the following information

- the nature of the breach
- the personal data compromised
- recommendations to the data subject concerning measures that the latter can adopt to protect his interests
- corrective actions implemented immediately, and
- the means by which the data subject may obtain more information in regard to the data breach.

ENFORCEMENT

The Law is of public order and of general observance throughout the Mexican Republic. It has the purpose of protecting personal data held by private parties, in order to require legitimate, controlled and informed processing, and ensure privacy and the right to informational self-determination of individuals.

Data subjects can enforce their ARCO Rights, when no response is obtained from the data controller via IFAI and ultimately the court system.

IFAI may act ex officio or in response to complaints regarding violations of the Law. If any breach of the Law or its Regulations is alleged, IFAI may perform on site inspection at the data controller's facilities to verify compliance with the Law.

Violations of the Law may result in monetary penalties or imprisonment.

- IFAI may impose monetary sanctions that go from 100 to 320,000 times the Mexico City minimum wage (currently $70.10 Mexican pesos; however, please note that the minimum wage is updated every year). With regard to violations committed concerning the processing of sensitive personal data, sanctions may be increased up to double the above amounts.
- Three months to three years imprisonment may be imposed on any person authorised to process personal data who, for profit, causes a security breach affecting the databases under its custody. Penalties will be doubled if the sensitive personal data is involved.
- Six months to five years imprisonment may be imposed on any person who, with the aim of obtaining unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or a person authorised to process such data. Penalties will be doubled if sensitive personal data is involved.

ELECTRONIC MARKETING

Email marketing constitutes the processing of persona data and is subject to the provisions of the Law, among them, the obligation to provide a Privacy Notice and request consent when needed.

ONLINE PRIVACY

The Regulations and Guidelines which address the use of cookies, web beacons and other analogous technologies, require that when a data controller uses online tracking mechanisms that permit the automatic collection of personal data, they provide prominent notice of: the use of such technologies; the fact that personal data is being collected; and the options to disable such technologies. The notice must also specify the type of personal data being gathered and the purpose of its collection.

An IP address alone may be considered personal data, however, there has not been a resolution or decision issued by the competent authority on this point.

KEY CONTACTS

Cecilia Azar
Partner
T +52 55.5261.1803
Cecilia.Azar@dlapiper.com

Paola Aldrete
Associate
T +52 55 5261 1888
Paola.Aldrete@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MONACO

Last modified 28 January 2015

LAW IN MONACO

Data protection in Monaco is regulated by Data Protection Law n° 1.165 of 23 December 1993, modified by Law n° 1.353 of 4 December 2008 ('DPL').

Furthermore, the Principally of Monaco is part of the Council of Europe and entered into Convention n° 108 of the European Council.

The Principality of Monaco is not part of the EU and as a consequence did not transpose Data Protection Directive 95/46/EC.

DEFINITIONS

Definition of personal data

Personal data is defined under the Data Protection Law as: *'data enabling identification of a determined or indeterminable person. Any individual who can be identified, directly or indirectly, notably by reference to an identification number or to one or more factors specific to his physical, psychological, psychological, economical, cultural, or social identity is deemed to be identifiable'.*

Definition of sensitive personal data

Sensitive personal data is not expressly defined under the DPL but it is deemed to be: *'Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health/genetic data, sex life, data concerning morals or social matters'.*

NATIONAL DATA PROTECTION AUTHORITY

The Monegasque regulator is the Commission for Control of Personal Data (*Commission de Contrôle des Informations Nominatives* or CCIN).

REGISTRATION

Data controllers who process personal data must inform/notify/request approval from the CCIN so that their processing of personal data may be registered. Any changes to the processing of personal data will require the registration to be amended.

The notification should include the following information:

- what data is being collected

- why the data will be processed
- the categories of data subject, and
- whether the data will be transferred either within or outside the Monaco.

DATA PROTECTION OFFICERS

There is no requirement in Monaco for organisations to appoint a data protection officer.

However, appointing a data protection officer is well perceived by the CCIN as evidence of the company's actions to ensure compliance with the data protection legislation; however, in practice, companies in Monaco do not appoint data protection officers in general.

COLLECTION & PROCESSING

Data processing must be justified by:

- data subject's consent
- a legal duty imposed to the data controller
- a public purpose
- completion of a contract entered into between the data controller and the data subject, or
- data controller's legitimate interest, subject not to fail to respect data subject's fundamental rights and liberties.

Where sensitive personal data is processed, one of the above conditions must be met plus one from an additional list of more stringent conditions.

The data controller must also provide the data subject with 'fair processing information'. This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

As the Principality of Monaco is not part of the EU, the DPL does not distinguish between EEA jurisdictions and non EEA jurisdictions.

However, the DPL provides that the transfer of data is authorised for cross border access, storage and processing of data only to a country with equivalent protection and reciprocity.

The CCIN has established a list of the countries deemed to have an equivalent protection and reciprocity. States, and parties to Convention of the Council of Europe n° 108 relating to the protection of individuals for personal data automatic processing, are deemed to have the equivalent protection as Monaco.

The declaration to CCIN should indicate whether it is intended for personal data to be transferred cross-border.

The transfer of data to countries that do not provide a sufficient level of protection shall be either:

- accepted by the data subject
- necessary for:

- safety of data subject's life
- the protection of public purpose
- compliance with obligations relating to the protection of a legal right
- public access to information
- completion of a contract entered into between the data controller and the data subject, or
- conclusion or completion of a contract entered into or to be entered into between the data controller and a third party in the interest of the data subject, or

- duly authorised by the CCIN under the condition that the data controller and the data recipient provide sufficient guarantees in order to protect fundamental rights and liberties.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm which might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data.

BREACH NOTIFICATION

There is no mandatory requirement in the DPL to report breaches or losses to the CCIN or to data subjects.

ENFORCEMENT

The CCIN and Monegasque Courts are responsible for enforcing the DPL. If the CCIN becomes aware that a data controller is in breach of the DPL, he can serve an enforcement notice requiring the data controller to rectify the position. Failure to comply with an enforcement notice is a criminal offence and can be punished on conviction of imprisonment of 1 to 6 months or a fine of from Eur 9,000 to Eur 90,000 or both.

ELECTRONIC MARKETING

Prior to implementing any electronic marketing activity the CCIN must be notified, as electronic marketing activities may use personal data. The law does not prohibit the use of personal data for the purpose of electronic marketing. However, when implementing electronic marketing activities a company must respect the provisions of article 1, article 10 and article 14 of the DPL.

The automated or non-automated processing of personal data must not infringe the fundamental rights and freedoms enshrined in Title III of the Constitution.

Personal data must be:

- collected and processed fairly and lawfully
- collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes
- adequate, relevant and not excessive in relation to the purposes for which it is collected and/ or further processed

- accurate and, if necessary, updated; every reasonable step must be taken to ensure that data which 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, and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

Processing of personal data must be justified:

- by consent from the data subject(s)
- by compliance with a legal obligation to which the data controller or their representative is subject
- by it being in the public interest
- by the performance of a contract or pre-contractual measures with the data subject, or
- by the fulfillment of a legitimate motive on the part of the data controller or their representative or by the recipient, on condition that the interests or fundamental rights and freedoms of the data subject are not infringed.

Persons from whom personal data is collected must be informed:

- of the identity of the data controller and, if applicable, the identity of their representative in Monaco
- of the purpose of processing
- of the obligatory or optional nature of replies
- of the consequences for them of failure to reply
- of the identity of recipients or categories of recipients
- of their right to oppose, access and rectify their data, and
- of their right to oppose the use on behalf of a third party, or the disclosure to a third party of their personal data for the purposes of prospection, particularly commercial prospection.

ONLINE PRIVACY

Prior to the use of Traffic Data, Location Data and Cookies the CCIN must be notified. The use of Traffic Data, Location Data and Cookies will have to respect of the provisions of the DPL.

In addition, the data controller or their representative must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss, corruption, unauthorised disclosure or access, in particular where processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Measures implemented must ensure an adequate level of security with regard to the risks posed by processing and by the nature of the data to be protected.

Where the data controller or their representative makes use of the services of one or more service providers, they must ensure that the latter are able to comply with the obligations laid down in the two previous paragraphs.

KEY CONTACTS

Gordon S. Blair Law Offices
gordonblair.com/

Genevieve Pace
Principal
T +377 93 25 00 52
genevieve.pace@gordonblair.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MONTENEGRO

Last modified 24 March 2015

LAW IN MONTENEGRO

The Montenegrin law governing data protection issues is the Law on Protection of Personal Data ('Official Journal of Montenegro', nos. 79/2008, 70/2009 and 44/2012) ('DP Law'). It originates from December 2008 and its latest amendments were made in August 2012.

DEFINITIONS

Defenition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person. The data subjects are natural persons whose identity is or can be determined, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Defenition of sensitive personal data

Under the DP Law, sensitive personal data is data relating to

- ethnicity, or race
- political opinion, or religious or philosophical belief
- trade union membership, and
- information on health condition and sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Agency for Protection of Personal Data and Free Access to Information ('DPA') is the local data protection authority. The DPA is seated in

Kralja Nikole 2
Podgorica
www.azlp.me

REGISTRATION

Each data controller is obliged firstly

1. to register itself as a data controller (this registration is to be performed only once), and, once the data controller's registration is completed

2. the controller has to register separately each database containing personal data ('Database') which it intends to establish, prior to the respective Database's establishment.

Both registrations are carried out by submitting the prescribed forms which are accessible on-line and can be submitted on-line, via the DPA's website (as identified in the section 'National Data Protection Authority'). The type and scope of the information necessary to be submitted to the DPA when registering the Database is explicitly prescribed by the DP Law (eg, the data controller's name and address of its registered seat, name of the Database, legal ground for the processing and processing's purpose, types of processed data, categories of data subjects, information on the data transfer out of Montenegro (if any), etc). Any subsequent significant change of the data processing should be registered with the DPA as well.

Exceptionally (ie if the intended data processing represents a special risk for rights and freedoms of natural persons), a data controller may, depending on the circumstances of each particular case, be obliged to obtain a prior DPA's approval for the respective processing (eg, if biometric data is to be processed and no data subject's consent is obtained for the respective processing).

DATA PROTECTION OFFICERS

Under the DP Law, a data controller is obliged, after the Database's establishment, to appoint a person responsible for the protection of personal data. However, this obligation is not applicable if a data controller has less than 10 employees who process personal data.

COLLECTION & PROCESSING

A precondition for the legitimate processing of personal data is so-called informed consent of the data subject. The content of this consent is explicitly prescribed by the DP Law (for example, data subjects have to be informed on the purpose of and legal ground for the respective processing). The processing is allowed without consent only exceptionally, ie in the particular cases explicitly prescribed by the DP Law (for example, if the processing is necessary for the fulfilment of the data controller's statutory obligations or for the protection of life and other vital interests of the data subject who cannot provide consent personally).

In any case, in order to be considered as fully compliant with the DP Law, the processing has to be done in a fair and lawful way, the type and scope of processed data must be proportionate to the purpose of the respective processing, the data should not be retained longer than necessary for the processing purpose's fulfilment and the data has to be true, complete and updated.

TRANSFER

Under the transfer rules envisaged by the DP Law, personal data may be transferred to countries or provided to international organizations, where adequate level of personal data protection is ensured, on the basis of the DPA's previsouly obtained consent. The DPA issues the respective consent only if it establishes that adequate measures for the protection of personal data are undertaken (the circumstances based on which the respective adequacy assessment is made include, for example, type of the data and statutory rules in force in the country to which the data is to be transferred).

However, the DPA's consent is not required for the data transfer out of Montenegro in certain cases explicitly prescribed by the DP Law (for example, if the data subject consented to the transfer and was made aware of possible consequences of such transfer or the data is transferred to the European Union or European Economic Area's country or to any country which is on the EU list of the countries which ensure adequate level of the data protection).

SECURITY

The DP Law prescribes that both data controllers and processors are obliged to undertake technical, personnel and organizational measures for the protection of personal data from loss, destruction, unauthorized access, alteration, publication and misuse. Furthermore, the natural persons who work on data processing are obliged to keep secrecy of

the processed personal data.

Additionally, data controllers are obliged to have internal rules on the personal data processing and protection (which should include the identification of the undertaken measures). The controllers should also determine which employees have access to the processed data (and to which of this data), as well as the types of data which may be provided to other users (and the conditions for the respective providing). Finally, if the processing is performed electronically, a data controller is obliged to ensure that certain information on the usage of the respective data and its users is automatically kept in the information system.

BREACH NOTIFICATION

There is no data security breach notification duty envisaged by the DP Law. However, the Law on Electronic Communications ('Official Journal of Montenegro', nos. 40/2013 and 56/2013) ('EC Law') does impose a duty on operators to notify, without delay, the Montenegrin Agency for Electronic Communications and Postal Activity ('EC Agency') and the DPA of any breach of personal data or privacy of the users. The respective users should be notified as well if the breach may have a detrimental effect to their personal data or privacy (unless the EC Agency issues an opinion that such notification is not needed). Failure to comply with any of the above duties is subject to offence liability and fines in range from EUR 6,000 to EUR 30,000 for a legal entity, and in range from EUR 300 to EUR 3,000 for a responsible person in a legal entity, plus, if some material gain was obtained by the offence's execution, the protective measure which includes the respective gain's seizure, may be imposed in addition to the above monetary fine.

ENFORCEMENT

The DPA is the authority competent for the DP Law's enforcement. It is authorized and obliged to monitor implementation of the DP Law, both *ex officio*, and upon a third party complaint.

When monitoring the DP Law's implementation, the DPA is authorized to pass the following decisions:

- order removal of the existing irregularities within certain period of time
- temporarily ban the processing of personal data which is carried out in contravention to the DP Law
- order deletion of illegally collected data
- ban transfer of data outside of Montenegro or its providing to data users which is carried out in contravention to the DP Law, and
- ban data processing by an outsourced data processor if it does not fulfil the data protection requirements or if its engagement as a data processor is carried out in contravention to the DP Law.

The DPA's decisions may not be appealed, but an administrative dispute before the competent court may be initiated against the same.

The DPA may also file a request for the initiation of an offence proceeding. The offences and sanctions are explicitly prescribed by the DP Law, which includes monetary fines in range from EUR 500 to EUR 20,000 for a legal entity and in range from EUR 150 to EUR 2,000 for a responsible person in a legal entity.

Moreover, criminal liability is also a possibility since a criminal offence Unauthorized collection and usage of personal data is prescribed by the Montenegrin Criminal Code. The sanctions prescribed for this criminal offence are a monetary fine (in an amount to be determined by the court) or imprisonment up to one (1) year. Both natural persons and legal entities can be subject to criminal liability.

ELECTRONIC MARKETING

Electronic marketing is not governed by the DP Law. Nevertheless, this law does govern protection of personal data

used in direct marketing. In that regard, it is prescribed that data subjects have to be provided with a possibility to oppose the processing of their personal data for the direct marketing purposes prior to the commencement of the respective processing. Regarding the usage of sensitive personal data in direct marketing, it is explicitly prescribed that a data subject's consent is a prerequisite for the respective processing.

Furthermore, although electronic marketing is not governed by the DP Law, there are other regulations which prescribe the rules relevant for the same including the Law on Electronic Trade ('Official Journal of the Republic of Montenegro', no. 80/04 and 'Official Journal of Montenegro', nos. 41/10, (…), 56/13) ('ET Law'). In this respect, one of the most important rules prescribed by the ET Law is the rule that any sending of unsolicited commercial messages is not allowed unless with prior consent of the persons to whom the respective marketing is addressed. It is absolutely forbidden to send any of the respective messages to the persons who have indicated that they do not want to receive the same (and a service provider which sends unsolicited commercial messages is obliged to establish a record of the respective persons). A violation of the respective rules is subject to offence liability and prescribed sanction is monetary fine in range from EUR 500 to EUR 17,000 (for a legal entity) and in range from EUR 100 to EUR 1,500 (for a responsible person in a legal entity). It is also prescribed that, in the case of particularly serious violations or repeated violations, a prohibition to perform business activity (lasting from three (3) months to six (6) months) may be imposed to an entity responsible for the respective violations.

ONLINE PRIVACY

There is no specific regulation explicitly governing on-line privacy (including cookies). Accordingly, the general data protection rules, as introduced by the DP Law, are, to the extent applicable, relevant for on-line privacy as well.

On the other hand, the EC Law, as defined in the section “Breach Notification” above, introduces relevant rules which are obligatory for the operators under this law. Among other, it is prescribed that a public electronic communication services' user is particularly entitled to the protection of his/her electronic communications' secrecy in compliance with the DP Law.

Furthermore, explicit rules on traffic data and location data are envisaged by the EC Law. Under these rules, the operators are:

1. *obliged to retain certain traffic data and location data for certain purposes explicitly prescribed by the law* (for example, for the detection and criminal prosecution of criminal offenders), whereas the retention period should last at least six (6) months and would not be longer than two (2) years ('Retention Obligation'), keeping in mind that this obligation does not apply to data which reveals a content of electronic communications

2. regarding *traffic data* related to subscribers/users which is not subject to the Retention Obligation, an operator is obliged to delete this data if it is no longer needed for the communication's transmission or can keep it, but only if it modifies the respective data in a way that it cannot be linked to a particular person. Apart from this, it is also prescribed that

    1. if traffic data's retention purpose is to use it for the calculation of the costs of the relevant services/interconnection, it can be retained for as long as claims regarding the respective costs can legally be requested, but under condition that an user is informed on its processing's purpose and duration, and that

    2. if traffic data's processing purpose is to promote and sell electronic communication services or to provide value added services, such processing is allowed, but only with the data subjects' prior consent (which can be withdrawn at any moment), and

3. regarding *location data* which is not subject to the Retention Obligation, an operator is allowed to process it but only with a data subject's consent (which can be withdrawn at any moment) or without the same if the respective data is modified in a way that it cannot be linked to a particular person.

Failure to comply with any of the above rules regarding the processing of traffic or location data which is not covered by the above-identified Retention Obligation, is subject to offence liability and fines in range from EUR 4,000 to EUR 20,000 for a legal entity, and in range from EUR 200 to EUR 2,000 for a responsible person in a legal entity.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Milena Rončević
Associate
T office +382 20 238 991
milena.roncevic@karanovic-nikolic.com

Sanja Spasenovic
Senior Associate
T Office +381 11 3094 200/ Direct T +381 11 3955 413
Sanja.Spasenovic@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

MOROCCO

Last modified 28 January 2015

LAW IN MOROCCO

Personal data protection is governed in Morocco by the Law n° 09-08 of 18 February 2009 relating to the protection of individuals with respect to the processing of personal data (the 'Law') and by its implementation Decree n° 2-09-165 of 21 May 2009 ('Decree').

DEFINITIONS

Definition of personal data

Personal data is defined by article 1.1 of the Law as any information of any nature and independently of its format, including the sound and images relating to an identified or identifiable individual, referred to in the Law as a 'concerned individual.' A person is deemed identifiable when he or she can be identified directly or indirectly, especially by reference to an identification number or one or several specific elements of his or her physical, physiological, genetic, psychological, economic, cultural or social identity.

Definition of sensitive personal data

Sensitive data is defined by article 1.3 of the Law as 'any information pertaining to a 'concerned individual' that reveals racial and ethnic origin, political, philosophical, religious opinions or trade union affiliation, or that concern sex life or health, including the genetic data.

NATIONAL DATA PROTECTION AUTHORITY

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel ('CNDP') (in English 'National Control Commission for the Protection of Personal Data')

6 *Boulevard Annakhil immeuble Les Patios*
3ème ètage
Hay Riad – Rabat, 10000 Morocco

T +212 537 57 11 24
F +212 537 57 21 41

contact@cndp.ma

REGISTRATION

The processing of personal data requires a prior notification to the CNDP.

The processing of sensitive data or of personal data that includes ID card numbers requires a prior authorisation from the CNDP.

The prior notification or authorisation application to the CNDP must specify, among other things:

- the purpose(s) of the processing
- the identity and the address of the data controller (ie the natural or legal person who determines the purpose and the means of the processing of the personal data and either implements such decisions itself or engages a data processor to implement them)
- the possible connections between databases
- the personal data processed and the categories of persons about whom personal data are processed
- the time period for which the data will be retained
- the department or person(s) in charge of implementing the data processing
- the recipients or categories of recipients of the personal data, and
- the measures taken to ensure the security of the processing. Additional specific security measures are required when processing sensitive data.

DATA PROTECTION OFFICERS

No requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Any personal data must be processed consistently with the following general principles:

- all personal data must be processed fairly and lawfully
- all personal data must be collected for specific, explicit and legitimate purposes and be subsequently processed in accordance with these purposes for which they are collected, and
- all personal data must be accurate, comprehensive and, when necessary, kept up to date.

The processing of personal data shall have received the individual's consent or shall fulfill one of the following conditions:

- processing is required by law
- the purpose of the processing is to save the individual's life
- the purpose of the processing is to carry out a public service
- the processing relates to the performance of a contract to which the concerned individual is a party, or
- the processing relates to achieving a legitimate interest of the data controller, balanced against the interests and fundamental rights and liberties of the concerned individual.

Where sensitive personal data are processed, a different list of specific conditions applies. Indeed, the concerned

individual must give his/her express consent for this processing unless the processing meets one of the following conditions:

- the processing is necessary for the exercise of legal or statutory functions of the controller
- the processing is necessary to protect the vital interests of the concerned individual, and that the concerned individual is in physically or legally incapable to give his/her consent
- the processing relates to data made public by the concerned individual, or
- the processing regards the recognition, exercise or defense of legal claims and is done exclusively for this purpose.

The person from whom the personal data is collected must receive notice of:

- the identity of the data controller and, if applicable, the data processor
- the purposes of the data processing; the recipients or categories of recipients of the data, and
- the right to object, for a legitimate reason, to the collection of such data, the right to access the collected data and the right to have the processed data rectified.

TRANSFER

The transfer of a data subject's personal data to another country is allowed if the country provides a sufficient level of protection in relation to an individuals' private life and fundamental rights and liberties. The sufficient nature of the protection is evaluated with regards to national laws and applicable security measures.

Data controllers may transfer personal data out of Morocco to countries that are not deemed to offer adequate protection if the transfer is necessary:

- to safeguarding the individual's life
- to safeguarding the public interest
- to comply with obligations relating to the recognition, exercise or defence of a legal right
- to the consultation of a public register intended to inform the public
- to the performance of a contract between the data controller and the individual, or pre-contractual measures undertaken at the individual's request, and
- to the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party.

SECURITY

The entity processing the data must take all reasonable precautions with regard to the nature of the data and the risk presented by the processing, in order to preserve the security of the data and, among other things, to prevent third parties gaining unauthorised access to such data. Where sensitive data are processed, the law sets forth specific security requirements that must be followed.

A data processor may only process personal data based upon the instructions of the data controller. The data processor must provide sufficient guarantees in terms of security and confidentiality. However, the data controller remains liable for

the processor's compliance with these obligations.

BREACH NOTIFICATION

The Law does not set out any obligation to notify the CNDP or the concerned individual in the event of a data security breach.

ENFORCEMENT

The CNDP is responsible for enforcing the Law.

Violations of the obligations set forth in the Law are punishable as an administrative and/or criminal offence.

Article 50 to 64 of the Law makes it a violation for any person intentionally to:

- fail to notify or seek CNDP's authorisation for data processing
- provide false information in the notification or in the applications for authorisation for the processing of personal data
- misappropriate or uses personal data in a manner incompatible with the purpose of the collection
- promote or carry an illegal collection of personal data, or
- fail to comply with the obligations set forth in the Law or the Decree.

The above offences are punishable by a fine ranging from MAD 10,000 (approx. US$1,200) to MAD 600,000 (approx. US$72,000) and/or imprisonment from three months to four years.

In addition, where the offender is a legal entity, it may be subject to the following penalties:

- partial seizure of its material goods
- seizure of objects and things whose production, use, carrying, holding or selling is an offence, and
- closure of the entity's premises where the offence was committed.

ELECTRONIC MARKETING

Article 10 of the Law provides that advertising/promotion via any electronic means (eg email, fax, SMS) is forbidden if the recipient has not affirmatively consented to it. However advertising and promotion are allowed when the data were collected directly from the recipient.

Unsolicited emails can only be sent without consent if:

- the contact details were provided in the course of a sale
- the marketing relates to a similar product, and
- the recipient was given a method to opt-out of the use of their contact details for marketing when they were collected.

In addition, the Law also prohibits the use of automated calling systems without the consent of the recipient.

Direct marketing emails may not disguise or conceal the identity of the sender. SMS marketing is also likely to be included within this prohibition on email marketing.

The restrictions on marketing by email only apply to email marketing sent to individuals and not to email marketing sent to corporations.

ONLINE PRIVACY

The Law does not specifically address the collection of location and traffic data by public electronic communications services providers, or the use of cookies (or similar technologies).

KEY CONTACTS

Hajji & Associés
www.ahlo.ma

Amin Hajji
Partner
T +212 522 48 74 74
a.hajji@ahlo.ma

Moulay El Amine EL HAMMOUMI IDRISSI
Senior Lawyer
T +212 522 48 74 74
moulay@ahlo.ma

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

NETHERLANDS

Last modified 28 January 2016

LAW IN NETHERLANDS

The Netherlands implemented the EU Data Protection Directive 95/46/EC on 1 September 2001 with the Dutch Personal Data Protection Act ('Wbp'). Enforcement is through the Dutch Data Protection Authority ('*Autoriteit Persoonsgegevens*').

DEFINITIONS

Definition of personal data

Any data relating to an identified or identifiable natural person.

Definition of sensitive personal data

Personal data regarding a person's religion or philosophy of life, race, political persuasion, health and sexual life, trade union membership, criminal behaviour and personal data regarding unlawful or objectionable conduct connected with a ban imposed as a result of such conduct.

NATIONAL DATA PROTECTION AUTHORITY

Autoriteit Persoonsgegevens
Juliana van Stolberglaan 4-10

2595 CL DEN HAAG
Postbox 93374
2509 AJ DEN HAAG

T 00.31.70 – 8888 500
F 00.31.70 – 8888 501

www.autoriteitpersoonsgegevens.nl

REGISTRATION

Unless an exemption applies, data controllers who process personal data by automatic means must notify the *Autoriteit Persoonsgegevens* so that their processing of personal data may be registered and made public. Changes to the processing of personal data will require the notification to be amended.

The notification shall, *inter alia*, include the following information:

- name and address of the data controller
- purpose(s) of the processing
- data subjects or categories of data subjects
- data or categories of data relating to these data subjects
- recipients or categories of recipients
- proposed transfers of personal data to countries outside the European Union, and
- a general description of the security measures the data controller is planning to take.

If any of the following changes occurs, the data controller must notify the *Autoriteit Persoonsgegevens* of these changes within one year after the previous notification. This concerns changes in:

- the purpose or purposes of the data processing
- the data subjects and recipients or categories of data subjects and recipients
- the security measures, and/or
- the intended transfers to countries outside the European Union.

However, this is only required if the changes are not of a purely incidental nature.

Also, any change to the name or address of the data controller should be notified to the *Autoriteit Persoonsgegevens* within one week.

DATA PROTECTION OFFICERS

Companies, industry associations, governments and institutions can appoint a data protection officer. There is no legal requirement in the Netherlands to do so. The data protection officer ensures that processing of personal data will take place in accordance with the Wbp. The statutory duties and powers of the data protection officer gives this officer an independent position within the organisation.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

For collecting personal data:

Pursuant to the Wbp, a data controller may only collect personal data if he has a purpose for this.

The purpose must be:

- specified
- explicit
- legitimate.

A data controller may not collect data if he has not clearly specified the purpose.

For processing personal data:

- the data subject has unambiguously given his prior consent thereto
- the processing is necessary for the performance of a contract to which the data subject is party
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject
- the transfer is necessary in order to protect the vital interests of the data subject
- the transfer is necessary or legally required in order to protect an important public interest
- the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data is supplied, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

In addition, personal data may not be further processed in a way incompatible with the purposes for which the data were originally collected. Whether further processing is incompatible depends on different circumstances, such as:

- the relationship between the purpose of the intended processing and the purposes for which the data originally was obtained
- the nature of the data concerned
- the consequences of the intended processing for the data subject
- the manner in which the data have been obtained
- the extent to which appropriate guarantees have been put in place with respect to the data subject.

Also, personal data may only be processed, where, given the purposes for which they are collected or subsequently processed, they are adequate, relevant and not excessive.

Finally, the Wbp sets out strict rules in relation to sensitive data. The main rule is that such data may not be processed, unless the data subject has given its explicit consent to it. However, there are exemptions to this rule which may apply in certain circumstances.

TRANSFER

Transfer of a data subject's personal data to non EU/European Economic Area countries is allowed if the countries provide 'adequate protection'.

Data controllers may transfer personal data out of the European Economic Area to countries which are not deemed to offer adequate protection if any of the following exceptions apply:

- the data subject has unambiguously given its consent thereto
- the transfer is necessary for the performance of the contract between the data controller and the data subject
- the transfer is necessary in respect of an important public interest, or for the establishment, exercise or defence in law of any right
- the transfer is necessary in order to protect the vital interests of the data subject
- the transfer occurred from a register that was set by law and can be consulted by anyone or by any person demonstrating a legitimate interest

- the transfer is based on unchanged Model Clauses as referred to in article 26(4) 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, or
- a permit thereto has been granted by the Minster of Justice, after consultation of the *Autoriteit Persoonsgegevens*. In order to obtain such permit, certain conditions should be met. One of these conditions can be implementing Binding Corporate Rules ('BCR').

BCR are internal codes of conduct regarding data privacy and security, to ensure that transfers of personal data outside the European Union will take place in accordance with the EU rules on data protection.

The use of BCRs is not obligatory. It will however bring benefits to both processors and controllers.

Once BCRs are approved they can be used by the controller and processor, thereby ensuring compliance with the EU data protection rules without having to negotiate the safeguards and conditions each and every time a contract is entered into.

SECURITY

Data controllers and processors must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

BREACH NOTIFICATION

Since 1 January 2016, a data breach, i.e. any security incident that leads or may lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed, must be reported to the *Autoriteit Persoonsgegevens*, of such data breach has or may have serious disadvantageous consequences for the protection of personal data.

In addition, data subjects need to be informed about a data breach if such data breach is likely to have unfavourable consequences to their privacy.

ENFORCEMENT

In the case of possible violations of the Wbp, the Autoriteit *Persoonsgegevens* can impose the following sanctions:

- enforce an administrative order; the data controller would be forced to change its policy with immediate effect; or
- administrative fines up to a maximum of EUR 820,000 or 10% of the annual turnover of the previous year may be imposed by the *Autoriteit Persoonsgegevens* in case of violation of the Wbp.

ELECTRONIC MARKETING

Electronic marketing is partially regulated in Article 11.7 of the Dutch Telecommunications Act ('Tw'). In the context of this Article electronic marketing could be defined as SMS, e-mail, fax and similar media for the purposes of unsolicited communication related to commercial, charitable or ideal purposes without the individuals' prior express consent.

Electronic marketing directed to corporations does not require prior consent if:

- the advertiser/electronic marketer uses electronic address data which are meant to be for this particular purpose, and
- if the individual is located outside the EU, the advertiser/electronic marketer complies with the relevant rules of that particular country in this respect.

On the basis of Article 11.7 of the Tw electronic marketing to individuals is in principle prohibited. If certain conditions

are being met, such as prior express consent, electronic marketing directly to individuals can be allowed. Furthermore, electronic marketing to individuals is also allowed if it is restricted to the marketing of existing customers and restricted to similar products/services of the advertiser/electronic marketer. In the last case, the advertiser/electronic marketer is obliged to provide opt-out possibilities to his customers when obtaining the data from the customers and in every marketing message sent.

ONLINE PRIVACY

Traffic Data

Traffic Data is regulated in Article 11.5 of the Tw. Traffic Data held by a public electronic communications services provider ('CSP') must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- it is being used to provide a value added service, and
- consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CSP for:

- the management of billing or traffic
- dealing with customer enquiries
- the prevention of fraud
- the provision of a value added service (subject to consent)
- market research (subject to consent)

Location Data

(Traffic Data not included) – Location Data is regulated in Article 11.5a of the Tw. Location Data may only be processed:

- if these data are being processed in anonymous form
- with informed consent of the individual

Cookie Compliance

The Netherlands implemented the E-Privacy Directive through the Dutch Telecommunications Act in Article 11.7a. (hereinafter: Article 11.7a). The Authority for Consumers and Markets ("ACM") is entrusted with the enforcement of Article 11.7a.

The main rule is that the website operator needs to obtain prior consent from a user before using cookies (opt in) and needs to clearly and unambiguously inform the user about these cookies (purpose, type of cookie, etc). Implicit consent is accepted under Dutch law. Please note that the website operator is entitled to refuse users access to its website(s) if no consent is given.

The requirement to obtain prior consent from a user does not apply in case of functional cookies analytic cookies that have little or no impact on the user's privacy (eg first party cookies).

The use of analytic cookies, affiliate or performance cookies used for the purpose of paying affiliates or cookies used for testing the effectiveness of certain banners) will be allowed without consent, on the condition that:

- the data collected by such cookies are not used for, among other things, creating profiles by the website owner and/or the third party with whom the data are shared; and
- website owners sharing the data with a third party take additional measures in order to limit any possible privacy impact.

The information collected through cookies are to be considered "personal data", unless the party which places the

cookies can prove otherwise. This goes only for tracking cookies, whereby the surfing behaviour of customers on several different websites is being observed (and the information obtained is being used for commercial purposes).

In case of violation of electronic marketing or online privacy legislation, the ACM can impose fines up to EUR 900,000 per violation.

KEY CONTACTS

Richard van Schaik
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +31 20 541 9828
richard.vanschaik@dlapiper.com

Robin de Wit
Of Counsel
T +31 20 5419674
robin.dewit@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

NEW ZEALAND

Last modified 26 January 2016

LAW IN NEW ZEALAND

The Privacy Act 1993 ('Act') governs how agencies collect, use, disclose, store, retain and give access to personal information. The Act gives the Privacy Commissioner the power to issue codes of practice that modify the operation of the Act in relation to specific industries, agencies, activities or types of personal information. Codes currently in place are:

- Credit Reporting Privacy Code
- Health Information Privacy Code
- Justice Sector Unique Identifier Code
- Superannuation Schemes Unique Identifier Code
- Telecommunications Information Privacy Code
- Civil Defence National Emergencies (Information Sharing) Code.

Enforcement is through the Privacy Commissioner.

DEFINITIONS

Definition of agency

'Agency' is defined under the Act as any person or body of persons, whether corporate or unincorporated, and whether in the public sector (including government departments) or the private sector. Certain bodies are specifically excluded from the definition.

Definition of personal data

Personal data is 'personal information' under the Act and is defined as information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.

Definition of sensitive personal data

Although no differentiation is made between how different types of personal information are to be treated under the Act, the codes of practice issued by the Privacy Commissioner may modify the operation of the Act for specific industries, agencies, activities and types of personnel information.

NATIONAL DATA PROTECTION AUTHORITY

The Privacy Commissioner's Office

Level 4
109-111 Featherston Street
Wellington 6143
New Zealand

T +64 474 7590
F +64 474 7595

enquiries@privacy.org.nz
www.privacy.org.nz

REGISTRATION

There is no obligation on agencies to notify the Privacy Commissioner that they are processing personal information. However, the Privacy Commissioner may require an agency to supply information for the purpose of publishing or supplementing a directory or to enable the Privacy Commissioner to respond to public enquiries in this regard.

The Privacy Commissioner may from time to time publish a directory of personal information including:

- the nature of any personal information held by an agency
- the purpose for which personal information is held by an agency
- the classes of individuals about whom personal information is held by an agency
- the period for which personal information is held by an agency
- the individuals entitled to access personal information held by an agency and the conditions relating to such access, and
- steps to be taken by an individual wishing to obtain access to personal information held by an agency.

DATA PROTECTION OFFICERS

The Act requires each agency to appoint within that agency, one or more individuals to be a privacy officer. The privacy officer's responsibilities include:

- the encouragement of compliance with the personal information privacy principles contained in the Act
- dealing with requests made to the agency pursuant to the Act
- working with the Privacy Commissioner in relation to investigations relating to the agency, and
- ensuring compliance with the provisions of the Act.

Provided the person appointed a privacy officer is within the agency, that person does not have to be a New Zealand citizen or reside in New Zealand.

Failure to appoint a privacy officer or obstructing or hindering the Privacy Commissioner is an offence under the Act. The maximum penalty on conviction is a fine of $2,000.

COLLECTION & PROCESSING

Subject to specific exceptions, agencies may collect, store and process personal information in accordance with the following 12 information privacy principles:

1. The personal information is needed for a lawful purpose connected with the agency's work.

2. The personal information is collected directly from the relevant person.

3. Before the personal information is collected, the agency has taken reasonable steps to ensure that the person knows that the information is being collected; the purpose for which it is being collected; the intended recipients; the name and address of the agency collecting and holding the information; if the information is authorised or required by law, the applicable law and the consequences if the requested information is not provided; and that the person concerned may access and correct the information.

4. The personal information is not collected in an unlawful or unfair way or in a way that unreasonably invades a person's privacy.

5. The personal information must be kept reasonably safe from being lost, accessed, used, modified or disclosed to unauthorised persons.

6. If the personal information is readily retrievable, the relevant person is entitled to know whether information is held and to have access to it.

7. The relevant person is entitled to request correction of the personal information. If the agency will not correct the information, the person may provide a statement of the correction sought to be attached to the personal information.

8. Before it is used, the agency must ensure that the personal information is accurate, up to date, complete, relevant and not misleading.

9. The personal information may not be kept for any longer than it is needed.

10. Subject to certain exceptions, personal information collected for one purpose may not be used for another purpose.

11. An agency must not disclose personal information to another person, body or agency except in specific circumstances.

12. An agency may only assign a unique identifier to an individual if it is needed for the agency to carry on its work efficiently and may not assign a unique identifier to an individual if the same identifier is used by another agency.

Personal information does not need to be collected directly from the relevant person if:

- the personal information is publicly available
- the relevant person authorises collection of the personal information from someone else
- non-compliance would not prejudice the interests of the relevant individual
- the personal information is being collected for a criminal investigation, enforcement of a financial penalty, protection of public revenue or the conduct of court proceedings

- compliance would prejudice the purpose of the collection of the personal information or is not practical in the circumstances, and
- the personal information will be used in a way which will not identify the person concerned.

TRANSFER

An agency should not disclose personal information to another entity unless the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained. Care must be taken that all safety and security precautions are met to ensure the safeguarding of that personal information to make certain that it is not misused or disclosed to any other party.

The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country ('State') by issuing a transfer prohibition notice ('Notice') if it is satisfied that information has been received in New Zealand from one State and will be transferred by an agency to a third State which does not provide comparable safeguards to the Act and the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines, which include:

- the collection limitation principle (there should be limits to the collection of personal data)
- the data quality principle (personal data should be accurate, complete and kept up to date)
- the purpose specification principle (the purposes for which personal data are collected should be specified)
- the use limitation principle (personal data should not be used otherwise than in accordance with the purpose specification principle, except with the consent of the data subject or by authority of law)
- the security safeguards principle (personal data should be protected by reasonable security safeguards)
- the openness principle (there should be a general policy of openness about developments, practices and policies relating to personal data)
- the individual participation principle (individuals should have the right to obtain confirmation of whether a data controller holds their personal data, to have that data communicated to him/her, to be given reasons if a request for that data is denied and to be able to challenge that denial, and to challenge data relating to him/her and have that data erased, rectified, completed or amended if successful), and
- the accountability principle (a data controller should be accountable for complying with the above principles).

In considering whether to issue a Notice, the Privacy Commissioner must have regard to whether the proposed transfer of personal information affects, or would be likely to affect any individual, the desirability of facilitating the free flow of information between New Zealand and other States, and any existing or developing international guidelines relevant to trans border data flows.

On 19 December 2012 the European Commission issued a decision formally declaring that New Zealand law provides a standard of data protection that is adequate for the purposes of EU law. This decision means that personal data can flow from the 27 EU member states to New Zealand for processing without any further safeguards being necessary.

Following the recent decision in the Schrems case, where the European Commission's decision to recognise the safe harbour agreement with the USA was invalidated, there have been calls to review New Zealand's adequacy status, primarily due to New Zealand's membership with the Five Eyes network. The USA safe harbour arrangement was one of six adequacy decisions issued by the Commission for countries outside the European Union of which another of those applies to New Zealand. However, to date this has not been acted upon by the European Commission.

SECURITY

An agency that holds personal information shall ensure that the information is kept securely and protected by such security safeguards as are reasonable in the circumstances to protect against:

- loss
- access, use, modification or disclosure, except with the authority of the agency, and
- other misuse or unauthorised disclosure.

If it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency must be done to prevent unauthorised use or unauthorised disclosure of the information.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report an interference with privacy.

Any person may make a complaint to the Privacy Commissioner alleging an action is, or appears to be, an interference with the privacy of an individual. For there to be an interference with privacy, there must be a breach of the law and the breach must lead to financial loss or other injury, an adverse effect on a person's right, benefit, privilege, obligation or interest or significant humiliation, loss of dignity or injury to a person's feelings. There is no requirement to show harm in a complaint about access to, or correction of, personal information. An unauthorised disclosure of personal information is sufficient to breach the Act.

ENFORCEMENT

In New Zealand, the Privacy Commissioner is responsible for investigating a breach of privacy laws. The Privacy Commissioner has powers to enquire into any matter if the Privacy Commissioner believes that the privacy of an individual is being, or is likely to be, infringed. The Privacy Commissioner will primarily seek to settle a complaint by conciliation and mediation. If a complaint cannot be settled in this way, a formal investigation may be conducted so that the Privacy Commissioner may form an opinion on how the law applies to the complaint. The Privacy Commissioner's opinion is not legally binding but is highly persuasive. The Privacy Commissioner is not able to issue a formal ruling or determination and cannot begin prosecution proceedings or impose a fine.

If the Privacy Commissioner is of the opinion that there has been an interference with privacy, the Privacy Commissioner may refer the matter to the Director of Human Rights who may then in turn decide to take the complaint to the Human Rights Review Tribunal. The Tribunal will hear the complaint afresh and its decision is legally binding.

ELECTRONIC MARKETING

The Act does not differentiate between the collection of and use of any 'personal information' for electronic marketing or other forms of direct marketing.

The Unsolicited Electronic Messages Act 2007:

- prohibits unsolicited commercial electronic messages (this includes email, fax, instant messaging, mobile/smart phone text (TXT) and image-based messages of a commercial nature – but does not cover internet pop-ups or voice telemarketing) with a New Zealand link (messages sent to, from or within New Zealand)
- requires commercial electronic messages to include accurate information about who authorised the message to be sent

- requires a functional unsubscribe facility to be included so that the recipient can instruct the sender not to send the recipient further messages, and
- prohibits using address-harvesting software to create address lists for sending unsolicited commercial electronic messages.

The Marketing Association of New Zealand has a code of practice for direct marketing which governs compliance by members of the principles of the code. The code establishes a 'Do Not Call' register to which anyone not wanting to receive any direct marketing can register.

ONLINE PRIVACY

Other than compliance with the Act, no additional legislation deals with the collection of location and traffic data by public electronic communications services providers and use of cookies (and similar technologies). The New Zealand Privacy Commissioner has general guidelines on protecting online privacy.

KEY CONTACTS

DLA Piper New Zealand
www.dlapiper.co.nz/

Brian Bray
Consultant
T +64 4 474 3236
brian.bray@dlapiper.co.nz

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

NIGERIA

Last modified 25 January 2016

LAW IN NIGERIA

Nigeria does not have a comprehensive legislative framework on the protection of personal data. However, there are a few industry-specific and targeted laws and regulations that provide some privacy-related protections, which include:

- The Constitution of the Federal Republic of Nigeria, 1999 (As Amended) ('the Constitution') which provides for the fundamental rights of its citizens and upholds the right of privacy as sacrosanct. Section 37 thereof provides for the guarantee and protection of the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.

- The Freedom of Information Act, 2011 ('FOI Act') which seeks to protect personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Also, Section 16 of the FOI Act provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege, health workers-client privilege, etc).

- The Child Rights Act No. 26 of 2003 (the 'Child Rights Act') regulates the protection of children (persons under the age of 18 years). This Act limits access to information relating to children in certain circumstances.

- The Consumer Code of Practice Regulations 2007 ('the NCC Regulations') issued by the regulator of the telecommunications industry in Nigeria, the Nigerian Communications Commission ('NCC'). The NCC Regulations provide that all licensees must take reasonable steps to protect customer information against improper or accidental disclosure, and must ensure that such information is securely stored and not kept longer than necessary. It also provides that customer information must not be transferred to any party except to the extent agreed with the Customer, as permitted or required by the NCC or other applicable laws or regulations.

- The National Information Technology Development Agency ('NITDA') which is the national authority responsible for planning, developing and promoting the use of information technology in Nigeria, and which issues the Guidelines on Data Protection ('NITDA Guidelines') pursuant to the NITDA Act 2007. The NITDA Guidelines prescribe guidelines for organisations that obtain and process personal of Nigeria residents and citizens within and outside Nigeria for protecting such personal data. The NITDA Guidelines apply to federal, state and local government agencies and institutions as well as private sector organisations that own, use or deploy information systems within the Federal Republic of Nigeria.

- The Cybercrimes (Prohibition, Prevention Etc) Act 2015 provides a legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act provides for the retention and protection of Data by financial institutions, criminalizes the interception of electronic communications etc.

DEFINITIONS

Definition of personal data

The NITDA Guidelines define personal data as any information relating to an identified or identifiable natural person ('data subject'); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address.

The Registration of Telephone Subscribers Regulation 2011 provides that personal information refers to:

- the full names (including mother's maiden name)
- gender
- date of birth
- residential address
- nationality
- state of origin
- occupation and such other personal information
- contact details of subscribers, as specified in the Registration Specifications.

Definition of sensitive personal data

The NITDA Guidelines define personal sensitive data as data relating to:

- religious or other beliefs
- sexual orientation
- health
- race
- ethnicity
- political views
- trade union membership
- criminal record.

NATIONAL DATA PROTECTION AUTHORITY

There is no specific authority bestowed with the responsibility of the protection of data, however sector specific regulatory agencies including NITDA, NCC etc provide services relating to the protection of data.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

The NITDA Guidelines provide that organisations should designate an employee as the Data Security Officer of that organisation whose duties shall include:

- Ensuring that the organization adheres to the stated policies
- Ensuring continued adherence to data protection and privacy policies and procedures
- Ensuring that individual data is protected
- Providing for effective oversight of the collection and use of individual information
- Being responsible for effective data protection and management within that organization; and ensuring

compliance with the privacy and data security policies

- Training and education for employees to promote awareness of and compliance with the privacy and data security policies
- Developing recommended practices and procedures to ensure compliance with the privacy and data security policies.

COLLECTION & PROCESSING

The collection and processing of personal data has to be done pursuant to the data subject's consent or as specifically provided by law. The NITDA Guidelines establish the scope of permitted collection and processing of personal data.

Collection

1. Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

2. Collection of personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, health or sex life can only be undertaken where:

- the data subject has given unambiguous consent
- the collection and processing is necessary for carrying out the obligations and specific function of the data controller in the field of employment
- the collection and processing is necessary to protect the interest of the data subject or another person where the data subject is incapable of giving consent
- the collection and processing relates to data which are manifestly made public by the data subject
- the collection and processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body and on the condition that the processing relates solely to its members or persons who have regular contact with it in connection with its purposes
- the collection and processing is necessary for the establishment, exercise or defence of legal claims.

3. Where data was not obtained from the data subject, the controller or third party should at the time of recording the personal data or if a disclosure to a third party is envisaged, provide the data subject no later than when the data are first disclosed with the following information (except where the data object already has it):

- the identity of the controller and of the representative (if any)
- the purposes of the processing
- any further information such as:
    - the categories of data concerned
    - the recipients or categories of recipients
    - the existence of the mechanism for access to and the mechanism to rectify the data concerning the data subject.

Processing

1. Personal data may be processed only if the data subject has given unambiguous consent and the processing is:

- necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- necessary for compliance with a legal obligation to which the controller is subject
- necessary to protect the interest of the data subject
- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or third party to whom the data are disclosed
- required for the purposes of management of health-care services subject to professional secrecy
- related to offences or criminal convictions
- necessary for legitimate interests pursued by the data controller or third party or parties to whom the data are disclosed, save where such interests are overridden by the interests or privacy of the data subject.

2. A complete register of criminal convictions is to be kept only under the control of official authority. Data relating to administrative sanctions or judgments in civil cases are to be processed under the control of official authority.

3. Every data subject shall be able to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to data subject are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed
- communication to the data subject in an intelligible form of the data undergoing processing and of any available information as to their source
- knowledge of the logic involved in any automatic processing of data concerning data subject at least in the case of the automated decisions
- rectification, erasure or blocking of data which does not comply with the provisions of the NITDA guidelines, in particular because of the incomplete or inaccurate nature of the data
- notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with these guidelines.

TRANSFER

The NCC Regulations provide that customer information must not be transferred to any party except to the extent agreed with the Customer, as permitted or required by the NCC or other applicable laws or regulations.

The NITDA Guidelines provide that personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection and where the controller finds that any country does not ensure an adequate level of protection of such personal data within the requirements of the Guidelines, the controller must prevent any transfer of data to the country in question. It further states that the following must be considered if a requirement exists to send or transfer data outside Nigeria:

- if the receiving country has adequate data protection legislation equivalent to that of Nigeria
- if it is necessary to send the data as part of the fulfilment of a contract

- if the data subject has consented
- if the data is being processed outside Nigeria by another office of the same firm which is established within Nigeria
- if there is a contract in place between the data controller and the receiving organisation which provides for the adequate protection of personal data.

The RTS Regulations make it mandatory for subscriber's information not to be transferred outside Nigeria.

SECURITY

To ensure the security of the data, the NITDA Guidelines provide that the data controller should implement technical and organizational measures to secure personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

BREACH NOTIFICATION

As far as we know, there is no mandatory legal requirement to report data security breaches or losses to the authorities or to data subjects.

Mandatory breach notification

Comments are the same as above.

ENFORCEMENT

Under the NCC Regulations, any licensee that contravenes any of the provisions of the Regulations would be in breach and would be liable to such fines, sanctions or penalties as may be determined by the Commission from time to time.

A breach of the NITDA Guidelines which was made pursuant to the NITDA Act 2007 would be considered a breach of the NITDA Act.

ELECTRONIC MARKETING

The NCC Regulations on Consumer Code of Practice provide that no Licensee shall engage in unsolicited telemarketing unless it discloses:

- at the beginning of the communication, the identity of the Licensee or other person on whose behalf it is made and the precise purpose of the communication
- during the communication, the full price of any product or service that is the subject of the communication
- that the person receiving the communication shall have an absolute right to cancel the agreement for purchase, lease or other supply of any product or service within seven (7) days of the communication, by calling a specific telephone number (without any charge, and that the Licensee shall specifically identify during the communication) unless the product or service has by that time been supplied to and used by the person receiving the communication.

Licensees are also required to conduct telemarketing in accordance with any 'call' or 'do not call' preferences recorded by the Consumer, at the time of entering into a contract for services or after, and in accordance with any other rules or guidelines issued by the Commission or any other competent authority.

The NCC Legal Guidelines for Internet Service Providers (ISP) provide that Commercial Communications ISPs must take reasonable steps to promote compliance with the following requirements for commercial email or other commercial

communications transmitted using the ISP's services:

- the communication must be clearly identified as a commercial communication
- the person or entity on whose behalf the communication is being sent must be clearly identified
- the conditions to be fulfilled in order to qualify for any promotional offers, including discounts, rebates or gifts, must be clearly stated
- promotional contests or games must be identified as such, and the rules and conditions to participate must be clearly stated
- persons transmitting unsolicited commercial communications must take account of any written request from recipients to be removed from mailing lists, including by means of public "opt-out registers" in which people who wish to avoid unsolicited commercial communications are identified.

The Nigerian Code of Advertising Practice Sales Promotion and other Rights/Restrictions on Practice provides that:

- All advertising and marketing communications directed to the Nigerian market using internet and other electronic media are subject to the laws regulating advertising practice in Nigeria.
- Without prejudice to any other restrictions or obligations imposed by the Act or under the code on advertising, all advertisements directed towards the Nigerian market using the Internet or any other electronic media must comply with the following requirements:
    - The commercial nature of the communication must not be concealed or misleading, it should be made clear in the subject header.
    - There should be clarity of the terms of the offer and devices should not be used to conceal or obscure any material factor such as: the price or other sale conditions likely to influence the customers' decision.
    - There should be clarity as to the procedure for concluding a contract.
    - Due recognition must be given to the standards of acceptable commercial behavior held by public groups before the posting of marketing communications to such groups using electronic media.
    - Unsolicited messages should not be sent except where there are reasonable grounds to believe that the consumers who received such communications will be interested in the subject matter or offer.
    - All marketing communications sent via electronic media should include a clear and transparent mechanism enabling the consumer to express the wish not to receive future solicitations.
- In addition to respecting the consumer's preferences, expressed either directly to the sender or through participation in a preference service programme, care should be taken to ensure that neither the marketing communication itself, nor any application used to enable consumers to open other marketing or advertising messages, interferes with the consumer's normal usage of electronic media.

ONLINE PRIVACY

The established rights of privacy (as guaranteed by the Constitution) apply equally to electronic media, such as mobile devices and the Internet. So, violations of these rights may be subject to civil enforcement. Furthermore the Cybercrimes (Prohibition, Prevention Etc) Act promotes cybersecurity, protects electronic communications and privacy rights.

KEY CONTACTS

Jackson, Etti & Edu
www.jacksonettiandedu.com

Koye Edu
Managing Partner
T (234) 01 461 7379 (234) 01 462 6842
koyeedu@jacksonettiandedu.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

NORWAY

Last modified 19 October 2015

LAW IN NORWAY

Being a member of the European Economic Area ('EEA'), Norway has implemented the EU Data Protection Directive 95/46/EC with the Personal Data Act (LOV-2000-04-14-31, below the 'Act') and the Personal Data Regulations (FOR-2000-12-15-1265, below the 'Regulations').

DEFINITIONS

Definition of personal data

Any information and assessments that may be linked to a natural person (the Act section 2, number 1).

Definition of sensitive personal data

Information relating to:

- racial or ethnic origin, or political opinions, philosophical or religious beliefs
- the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act
- health
- sex life, or
- trade union membership (the Act section 2, number 8).

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Authority (Nw: Datatilsynet, below the 'DPA')

Visiting address: Tollbugata 3, 0152 Oslo
Postal address: PO. Box 8177 Dep., NO-0034 Oslo

T +47 22 39 69 00
F +47 22 42 23 50

W www.datatilsynet.no
E postkasse@datatilsynet.no

REGISTRATION

The Act separates between obligations to submit notification to the DPA and obligations to obtain a license from the DPA. Certain types of processing of personal data are, however, neither subject to the notification obligation nor the license obligation. Thus, there is no general rule in Norway requiring all controllers to register with the DPA.

Examples of processing activities exempt from both the notification obligation and the license obligation:

- the processing of personal data concerning customers, subscribers and suppliers (as part of the administration and fulfilment of contractual obligations), cf. the Regulations section 7-7, and
- employers' standard processing of personal data relating to current or former employees, personnel, representatives, temporary manpower and applicants for a position, cf. the Regulations section 7-16.

Examples of processing activities subject to the notification obligation:

- video surveillance
- whistleblower schemes
- prize competitions, or
- compliance with legislation to combat money laundering.

Examples of processing activities subject to the license obligation:

- a license from the DPA is generally required for the processing of sensitive personal data, cf. the Act section 33, and
- controllers in certain business sectors are obligated to obtain a license, including:
  - providers of telecommunication services for the purpose of customer administration, invoicing and the provision of services in connection with the subscriber's use of the telecommunications network (cf. the Regulations section 7-1)
  - providers of insurance services for the purpose of customer administration, invoicing and the implementation of insurance contracts (cf. the Regulations section 7-2), and
  - banks and financial institutions for the purpose of customer administration, invoicing and the implementation of banking services (cf. the Regulations section 7-3).

DATA PROTECTION OFFICERS

There is no statutory requirement to appoint a Data Protection Officer ('DPO'). The DPA may pursuant to the Regulations section 7-12 consent to exemptions being granted from the obligation to submit notification pursuant to the Act, if the controller designates an independent privacy ombudsman (*Nw: Personvernombud*) who is responsible for ensuring that the controller complies with the Act and the Regulations. The main benefits are as follows:

- the controller will be exempt from the obligation to submit notifications pursuant to the Act and the Regulations
- the appointment of a DPO will build goodwill for and strengthen the controller's reputation with respect to privacy issues and processing of personal data (shows the controller's focus for privacy/processing compliance efforts), and
- the DPA's courses will maintain and strengthen the DPO's qualifications and skills within processing of personal data and general privacy issues.

The DPO is inter alia responsible for:

- ensuring that the controller complies with the Act and the Regulations
- maintaining an overview of the categories of personal data that are processed and the types of processing

- ensuring that the controller has implemented an internal control system
- being a contact person for the DPA
- addressing breaches of the Act and the Regulations
- keeping itself posted with respect to the trends and developments within privacy and applicable legislation, and
- assisting the data subjects and answering questions relating to the processing and privacy issues.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject consents
- there is statutory authority for the processing
- the processing is necessary to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract
- the processing is necessary to enable the controller to fulfil a legal obligation
- the processing is necessary to protect the vital interests of the data subject
- the processing is necessary to perform a task in the public interest
- the processing is necessary to exercise official authority, or
- the processing is necessary to enable the controller or third parties to whom the data is disclosed to protect a legitimate interest, except where such interest is overridden by the interests of the data subject.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of additional conditions.

Whichever of the above conditions is relied upon, the controller must first provide the data subject with certain information, unless an exemption applies. The notification shall include information on the identity of the controller, the purposes of the processing, whether the data will be disclosed and if so, the identity of the controller, the fact that the provision of data is voluntary and any other circumstances that will enable the data subject to exercise his rights pursuant to the Act.

TRANSFER

Personal data may pursuant to the Act section 29 only be transferred to countries which ensure an adequate level of protection of the data. There are, however, several exceptions from this point of departure. Personal data may pursuant to the Act section 30 also be transferred to countries which do not ensure an adequate level of protection if:

a. the data subject has consented to the transfer
b. there is an obligation to transfer the personal data pursuant to an international agreement or as a result of membership of an international organisation
c. the transfer is necessary for the performance of a contract with the data subject, or for the performance of tasks at the request of the data subject prior to entering into such a contract

d. the transfer is necessary for the conclusion or performance of a contract with a third party in the interest of the data subject

e. the transfer is necessary in order to protect the vital interests of the data subject

f. the transfer is necessary in order to establish, exercise or defend a legal claim

g. the transfer is necessary or legally required in order to protect an important public interest, or

h. there is statutory authority for demanding data from a public register.

The DPA may allow transfer even if the conditions set out above are not fulfilled if the controller provides adequate safeguards with respect to the protection of the rights of the data subject, such as transfers:

- subject to the EU Model Clauses and approved by the DPA before the transfer
- pursuant to Binding Corporate Rules approved by the DPA, and
- to Safe Harbour certified entities in the USA.*

Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.

SECURITY

Data controllers and processors shall by means of planned, systematic measures ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data.

BREACH NOTIFICATION

Data security breaches which have resulted in the unauthorised disclosure of personal data where confidentiality is necessary, is subject to notification to the DPA. DPA guidance and practice indicates that data subjects may need to be notified provided the discrepancy may be detrimental to the interests of the data subject (eg identity theft, forgery, harassment).

ENFORCEMENT

The DPA is responsible for enforcement of the Act and DPA's decisions may be appealed to the Privacy Appeals Board (Nw: *Personvernnemnda*).

Sanctions and remedies for non-compliance:

- change/cease unlawful processing (the Act section 46): The DPA may order that processing of personal data in violation of the provisions in or pursuant to the Act shall cease, or impose conditions which must be met in order for the processing to comply with the Act
- data offence fine (the Act section 46): The DPA may issue orders to the effect that violation of provisions laid down in or pursuant to the Act shall result in a data offence fine of maximum 10 times the National Insurance Basic Amount. The National Insurance Basic Amount is regulated yearly and has since 1 May 2013 been NOK 85 245. Thus, the maximum data offence fine is per January 2014 NOK 852 450 (≈ EUR 100 000)
- coercive fines (the Act section 47): For certain breaches, the DPA may also impose a coercive fine which will run for each day from the expiry of the time limit set for compliance with the order until the order has been complied

with

- penalties (the Act section 48): Anyone who wilfully or through gross negligence violates certain provisions in the Act, shall pursuant to the Act section 48 be liable to fines or imprisonment for a term not exceeding one year or both. In particularly aggravating circumstances, a sentence of imprisonment for a term not exceeding three years may be imposed. An accomplice shall be liable to similar penalties, and/or

- compensation (the Act section 49): The controller shall compensate damage suffered as a result of the fact that personal data have been processed contrary to provisions laid down in or pursuant to the Act, unless it is established that the damage is not due to error or neglect on the part of the controller. The compensation shall be equivalent to the financial loss incurred by the injured party as a result of the unlawful processing. The controller may also be ordered to pay such compensation for damage of a non-economic nature (compensation for non-pecuniary damage) as seems reasonable.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act).

Pursuant to the Marketing Control Act (Nw: *Markedsføringsloven*) section 15, it is prohibited in the course of trade, without the prior consent of the recipient, to send marketing communications to natural persons using electronic methods of communication which permit individual communication, such as electronic mail, telefax or automated calling systems (calling machines).

Prior consent is however not required for electronic mail marketing where there is an existing customer relationship and the contracting trader has obtained the electronic address of the customer in connection with a sale. The marketing may only relate to the trader's own goods, services or other products corresponding to those on which the customer relationship is based.

At the time that the electronic address is obtained, and at the time of any subsequent marketing communication, the customer shall be given a simple and free opportunity to opt out of receiving such communications.

'Electronic mail' in the context of the Marketing Control Act means any communication in the form of text, speech, sound or image that is sent via an electronic communications network, and that can be stored on the network or in the terminal equipment of the recipient until the recipient retrieves it. This includes text and multimedia messages sent to mobile telephones.

Direct marketing emails must not conceal or disguise the identity of the sender. If the email is unsolicited, it shall clearly state that the email contains a marketing message upon receipt of the message (The Norwegian E-commerce Act, Nw: *Ehandelsloven*, section 9).

ONLINE PRIVACY

Traffic Data

Traffic data is defined in Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services (Nw: *Ekomforskriften* F16.02.2004 nr 401) section 7-1 as data which is necessary to transfer communication in an electronic communications network or for billing of such transfer services.

Processing of traffic data held by a Communications Services Provider ('CSP') (Nw: *Tilbyder*) may only be performed by individuals tasked with invoicing, traffic management, customer enquiries, marketing of electronic communications networks or the prevention or detection of fraud.

Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication (Electronic Communications Act section 2-7 (Nw: *Ekomloven*). However, Traffic Data

can be retained if it is being used to provide a value added service and consent has been given for the retention of the Traffic Data.

Location Data

Location data may only be processed subject to explicit consent for the provision of a value added service which is not a public telephony service, and the users must be given understandable information on which data is processed and how the data is used. The user shall have the opportunity to withdraw their consent. See Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services section 7-2.

Cookie Compliance

The Electronic Communications Act has been changed in accordance with directive 2009/136/EC regarding the use of cookies. According to section 2-7 b, the user must give their consent before cookies or any other form of data is stored in their browser. The users must receive clear and comprehensive information about the use of cookies and the purpose of the storage or access. However, obtaining user consent is not required if the cookie solely has the purpose of transferring communication in an electronic network, or if it is deemed to be necessary for the delivery of a service requested by the user. The user's consent to processing may be expressed by using the appropriate settings of a browser or other application. Where the use of a cookie involves processing of personal data, the service providers will have to comply with the additional requirements of the Data Protection Act.

KEY CONTACTS

Cecilie Rønnevik
Lawyer - Advokatfullmektig
T +4724131540
Cecilie.Ronnevik@dlapiper.com

Petter Bjerke
Partner
T T +47 2413 1654
petter.bjerke@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

PAKISTAN

Last modified 28 January 2015

LAW IN PAKISTAN

There is, at the date of publication, no legislation regulating the protection of data in Pakistan.

DEFINITIONS

Definition of personal data

In the absence of any legislation regulating the protection of data in Pakistan, the term 'personal data' is undefined.

Definition of sensitive personal data

In the absence of any legislation regulating the protection of data in Pakistan, the term 'sensitive personal data' is undefined.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Pakistan.

REGISTRATION

Data controllers or collectors do not need to register with any authority.

DATA PROTECTION OFFICERS

Organisations in Pakistan are not required to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers can collect and process personal data under any conditions.

TRANSFER

Although the transfer of data to third parties is not specifically regulated under the laws of Pakistan, data cannot be transferred from Pakistan to a country which is not recognised by Pakistan. Pakistan currently does not recognise Israel, Taiwan, Somaliland, Nagorno Karabakh, Transnistria, Abkhazia, Northern Cyprus, Sahrawi Arab Democratic Republic, South Ossetia and Armenia. This list may change from time to time. Furthermore, data can only be transferred to India if such a transfer can be justified by the transferor.

Besides being regulated by contractual terms, data collated by*, inter alia*, banks, insurance firms, hospitals, defence

establishments and other 'sensitive' installations/institutions cannot be transferred to any individual/body unless it is transferred with the permission of the relevant regulator or similar bodies on a confidential basis. Additionally, in certain cases data cannot be transferred without the permission of the relevant client/customer.

Please note however that in the case of banks/ financial institutions, the secrecy of banking transactions must be maintained.

SECURITY

Data controllers do not have to fulfil any security requirements.

BREACH NOTIFICATION

Data security breaches or losses do not have to be reported or notified to any body or individual.

ENFORCEMENT

In the absence of any legislation in the sphere of data protection no body or entity enforces any law. Enforcement and appropriate relief may however be sought through courts of law having jurisdiction in the matter.

ELECTRONIC MARKETING

There is, at the date of publication, no subsisting legislation regulating electronic marketing in Pakistan. Please note that an earlier law promulgated in this regard has since lapsed.

ONLINE PRIVACY

There is, at the date of publication, no subsisting legislation regulating online privacy in Pakistan. Please note that an earlier law promulgated in this regard has since lapsed.

KEY CONTACTS

Liaquat Merchant Associates
www.liaquatmerchant.com

Darakhshan Sheikh Vohra
Partner
T +9221 3583 5101 – 104
d.vohra@liaquatmerchant.com

Saqiba Akhlaq Khan
Associate
T +9221 3583 5101 – 104
s.akhlaq@liaquatmerchant.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

PANAMA

Last modified 26 January 2015

LAW IN PANAMA

In recent years, Panama has taken significant legislative steps to regulate electronic data protection and internet commerce. However, this regime remains a work in progress.

The primary laws and regulations thus far enacted are Law 51 of 22 July 2008, as amended by Law 82 of 9 November 2012 ('Law 51'), and Executive Decree No. 40 of 19 May 2009 ('Decree 40'). The central purpose of both Law 51 and Decree 40 is to regulate the creation, utilization and storage of electronic documents and signatures in Panama, through a registration process and the supervision of providers of data storage services. Law 51 and Decree 40 provide for enforcement through the General Directorate of Electronic Commerce (*Dirección General de Comercio Electrónico*) ('DGCE').

DEFINITIONS

Definition of personal data

Personal Data is not expressly defined under Panamanian law. However, it is generally deemed to include information that can specifically identify an individual, such as one's name, postal address (including billing and shipping addresses), telephone number, e-mail address, credit card number, or a username.

Definition of sensitive personal data

'Sensitive Personal Data' is not defined under Panamanian Law.

NATIONAL DATA PROTECTION AUTHORITY

The General Directorate of Electronic Commerce
(*Dirección General de Comercio Electrónico*)

Plaza Edison, Sector El Paical, Floors 2 & 3.

T (507) 560-0600
(507) 560-0700
F (507) 261-1942

contactenos@mici.gob.pa

REGISTRATION

Under Decree 40, electronic data storage companies and companies engaged in online electronic signature verification

must register with the DGCE. For companies otherwise engaged in e-commerce-related activities, registration with the DGCE is voluntary and can be completed online and free of cost. Registration must occur no later than 15 days prior to the commencement of data processing activities and shall include, *inter alia*, the following information:

- name of the company
- company´s physical address, telephone and fax number
- legal representative of the company
- company´s internet address or URL
- contact email provided by company to customers
- public Registry and Ministry of Commerce Registration Information
- in the event that an undertaken activity requires specific authorization or permits, evidence thereof
- tax Identification Number
- description of services offered by the company, including pricing information and applicable taxes, and
- the Company's code of conduct.

Law 51 and Decree 40 set forth certain additional registration requirements for companies that are engaged in each of the activities for which registration is mandatory.

Further, pursuant to recently enacted regulations, individuals or entities who wish to electronically interact with government entities must first register by activating a user account and executing a release form that is available both physically and online. To the extent necessary, government entities may also request a petitioner´s consent to access such petitioner's personal information that is available on a different government entity´s system.

DATA PROTECTION OFFICERS

Appointment of a data protection officer is not required.

COLLECTION & PROCESSING

In Panama, personal information is protected at the constitutional level. The Constitution provides that any person or entity that obtains personal information and/or personal documents, either from a person or a company who provides such information willingly, or through any other means, may not disclose such information *without the consent of its lawful owner (there is no specific definition or explanation of who is considered the 'lawful owner' of personal information)*. An exception to the consent rule is the disclosure of such information pursuant to a valid judicial or governmental request.

The disclosure of personal information without consent is also prohibited by the Panamanian Criminal Code. Criminal penalties apply to the disclosure of personal information when the disclosure causes harm to the information's lawful owner. Law 51 specifically establishes that this criminal law prohibition applies to electronically stored information.

Panamanian law further requires that providers of online data storage services take reasonable measures to ensure that company personnel who come into contact with confidential information do not have a criminal record, have obtained the necessary technical skills to handle such data and information, and possess reasonable knowledge of existing legal

restrictions related to the disclosure of such information. Although this prohibition is specifically intended to apply to entities that provide online data storage services, it is not unforeseeable that it could also be construed to apply to any company engaged in e-commerce.

TRANSFER

Although the Panamanian e-commerce regulatory framework is not yet fully developed, the existing regulations follow the constitutional principle that the consent of the lawful owner is required for the transfer of any personal information.

Pursuant to Law 51, when a customer provides his email address during the process of acquiring or subscribing to a service offered online, the company providing such service must disclose to the customer its intent to use the email address in the future for commercial communications and, further, must obtain the customer's express consent for such purposes.

The client or customer must also be able to revoke such consent easily, through a simple process made available by the provider of the service.

While the manner in which this restriction appears to have been drafted suggests that it applies exclusively to online service providers, its broader application to all companies that sell products online or are engaged in e-commerce activities is foreseeable.

SECURITY

Decree 40 establishes certain security requirements applicable only to electronic data storage and electronic signature verification companies, for whom registration with the DGCE is mandatory. The main requirements are adherence to the security parameters periodically published by the DGCE, and the performance of annual self-audits, the results of which must be filed with the DGCE in order for the company to renew its registration. In addition, these companies must create a disaster recovery plan that allows such providers to re-establish regular operations within twelve hours of the occurrence of a disruptive event.

No similar provisions have been enacted with respect to companies who engage in other types of e-commerce, ie, those for whom registration is voluntary.

BREACH NOTIFICATION

Law 51 does not require breach notification.

ENFORCEMENT

The DGCE is responsible for enforcement of the existing e-commerce and related regulations, including the publication of additional complementary regulations. Sanctions include the suspension or permanent ban of the activities of companies that infringe certain regulations, as well as fines of up to US$150,000.

ELECTRONIC MARKETING

With respect to email advertising, Panamanian law requires that all such emails:

- state that they are commercial communications
- include the name of the sender, and
- set forth the mechanism through which the recipient may choose not to receive any further communications from the particular sender. These requirements apply to other promotional offers as well.

Further, although opt-out tools are not prohibited, the client's initial opt-in consent is specifically required to use the client's email for advertising purposes. Further, although no specific prohibition has been enacted with respect to the

use of information for online advertising, obtaining the customer's consent is always preferable.

ONLINE PRIVACY

The existing regulatory framework does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Galindo, Arias & Lopez
gala.com.pa/

Diego Herrera
T +507 303 0303
dherrera@gala.com.pa

James Sattin
T +507 303 0303
jsattin@gala.com.pa

Jose Luis Sosa
T +507 303 0303
jsosa@gala.com.pa

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

PERU

Last modified 27 January 2016

LAW IN PERU

Personal data protection is governed in Peru by:

- the Personal Data Protection Law No. 29733 ('PDPL') published on July 3, 2011
- its regulations enacted by Supreme Decree 003-2013-JUS and published on March 22, 2013 (the 'Regulations'), and
- the Security Policy on Information Managed by Databanks of Personal Data enacted by Directorial Resolution N° 019-2013-JUS/DGPDP on October 11, 2013.

Although several provisions of the PDPL have been in force since July 4, 2011, most of the provisions of the PDPL only came into force on May 8, 2013 (30 business days after the issuance of the Regulations).

DEFINITIONS

Definition of personal data

The term “personal data” is defined broadly under the PDPL and its Regulations as all numerical, alphabetical, graphic, photographic, sound, or any other type of information concerning an individual which identifies or could be used to identify the individual through reasonable means.

Definition of sensitive personal data

“Sensitive data” is defined under the PDPL and its Regulations as biometric data which can identity someone; racial and ethnic background; income; political or religious opinions or creed; union membership; data related to health or sexual orientation and, in general, physical, mental and emotional characteristics, facts or circumstances of emotional or family life, and personal habits corresponding to the most intimate sphere of private life.

NATIONAL DATA PROTECTION AUTHORITY

The General Agency on Data Protection (Agency), part of the Ministry of Justice and Human Rights, is the National Authority for the Protection of Personal Data. The Agency oversees the PDPL.

Scipión Llona Nº 350, Miraflores
Lima, Peru
T +511 204 8020 (annex 1030)
www.minjus.gob.pe/proteccion de datos personales

REGISTRATION

Public and private databases containing personal data must be registered with the National Registry for Personal Data Protection. The following items shall also be registered in the Registry:

- codes of conduct, if any, that set standards for the processing of personal data, which are designed to ensure and improve the operation of information systems (the preparation of these codes by the owner or user of a database is voluntary)
- penalties, injunctive relief or remedies imposed by the Agency, and
- communications to the agency regarding cross-border transfers.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

The collection and processing of personal data requires the prior, informed, express and unequivocal consent of the data subject. Consent may be expressed electronic means.

'Sensitive data' requires, additionally, that the data subject's consent be expressed in writing.

The consent of the data subject is not necessary when:

- the data are compiled or transferred for the fulfilment of governmental agency duties
- the data are contained or destined to be contained in a publicly available source
- the data are related to credit standing and financial solvency, as governed by applicable law (Law No. 27489)
- a law is enacted to promote competition in regulated markets, under the powers afforded by the Framework Law for Regulatory Bodies of Private Investment on Public Services (Law No. 27332), provided that the information supplied does not breach the user's privacy
- the data are necessary for a contractual, scientific or professional relationship with the data subject, provided that such data is necessary for the development and compliance with such relationship
- the data are needed to protect the health of the data subject, and data processing is necessary, in circumstances of risk, for prevention, diagnosis, and medical or surgical treatment, provided that the processing is carried out in health facilities or by professionals in health sciences observing professional secrecy
- the data are needed for public interest reasons declared by law or public health reasons (both must be declared as such by the Ministry of Health) or to conduct epidemiological studies or the like, as long as dissociation procedures are applied
- the data are dissociated or anonymized
- the data are used by a non-profit organization with a political, religious, or trade union purpose, and refer to the data of its members within the scope of the organization´s activities
- the data are necessary to safeguard the legitimate interest of the data subject or the data handler, or
- the data are used for other purposes recognized as exempt in law or in the Regulations.

TRANSFER

The transfer of personal data is subject to substantially the same restrictions as those applicable to collection and

processing. Under the Regulations, a data transfer requires the consent of the data subject. The recipient of the data must assume the same obligations as the owner of the personal data.

However, in the case of cross-border transfers, the data holder generally must abstain from making transfers of personal data if the destination country does not afford 'adequate protection levels', which are equivalent to those afforded by the PDPL or in international standards.

If the destination country fails to offer 'adequate protection levels', the sender of the cross-border transfer of personal data must guarantee that the treatment of personal data meets 'adequate protection levels'. Generally, 'adequate measures' can be ensured via a written agreement that requires that the data will be protected in accordance with the requirements of the PDPL.

This guarantee is not necessary in the following cases:

- in accordance with international treaties in which Peru is a party
- international Judicial cooperation
- international cooperation among intelligence agencies to combat terrorism, drug trafficking, money laundry, corruption, human trafficking and other forms of organized crime
- when necessary for a contractual relationship with the data subject, or for a scientific or professional relationship
- bank or stock transfers concerning transactions in accordance with the applicable law
- cross border transfers performed to protect, prevent, diagnose or medically or surgically treat the data subject, or to perform studies of epidemiology or the like, provided a data dissociation procedure has been applied
- the owner of the personal data has given its prior, informed, express and unequivocal consent to the transfer, or
- other exempt purposes established by the Regulations.

As with domestic transfers, the recipient must assume the same obligations as the owner of the personal data.

SECURITY

Database holders and data handlers must adopt technical, organizational and legal measures necessary to guarantee the security of the personal data they hold. The measures taken must ensure a level of security appropriate to the nature and purpose of the personal data involved.

The Agency has passed a Directive regarding the security standards to which the processing of personal data must be subject. This Directive establishes different standards depending on the features of the database. The features that are relevant are the:

- number of data subjects whose data are contained in the database
- number of fields of the database (for example, name, address, phone number)
- existence of sensitive data, and
- owner of the database (an individual or entity).

BREACH NOTIFICATION

Under section 2.3.4.2 of the Security Policy on Information Managed by Databanks of Personal Data, enacted by Directorial Resolution N° 019-2013-JUS/DGPDP on October 11, 2013, the databank owner must inform the data subject of 'any incident that significantly affects their property or their moral rights', as soon as the occurrence of the incident is confirmed. Thus, certain data breaches trigger notice obligations. The minimum information to be provided in a notice includes:

- a description of the incident
- disclosed personal data
- recommendations to the data subject, and
- implemented corrective measures.

On the other hand, no breach notification to the General Agency on Data Protection is required.

ENFORCEMENT

The Agency is the government entity entrusted with enforcing the provisions of the PDPL. A breach of the obligations set forth therein gives rise to penalties.

The sanctions that could be imposed for breaching data protection standards vary depending on the nature or magnitude of the offense.

- The fine applicable to ordinary infringements ranges from approximately USD 686 to USD 6,859.
- The fine applicable to severe infringements ranges from approximately USD 6,859 to USD 68,592.
- The fine applicable to very severe infringements ranges from approximately USD 68,592 to USD 137,184.

It should be noted that notwithstanding the abovementioned amounts, in no scenario may a fine be greater than 10% of the alleged offender's gross revenues or earnings for the immediately preceding year.

The Agency is also authorized to resort to “coactive fines” which amount shall not exceed approximately USD 14,513. Coactive fines are those that are imposed in addition to the above mentioned fines if the offender, despite being found liable and sanctioned as a consequence thereof, fails to remedy the unlawful practice.

The above sanctions are applicable in addition to civil (e.g. damages) and criminal liability (eg breach of professional secrecy) that may arise pursuant to breaches of the PDPL.

ELECTRONIC MARKETING

The PDPL does not expressly regulate electronic marketing. However, the PDPL will apply to electronic marketing activities when personal data is processed as a result.

Separately, the 'Anti Spam Law' No. 28493 and its regulations (Supreme Decree No. 031-2005-MTC) regulate specific aspects of electronic marketing.

These laws are applicable to any electronic mail message that originates in Peru and that qualifies as unsolicited commercial e-mail – defined broadly as e-mail that contains promotional commercial information regarding goods and services, including information regarding events, competitions and/or activities, traded, offered, sponsored or organized by company individuals.

Unsolicited commercial e-mails must contain:

- The word *PUBLICIDAD* (which means advertisement) at the beginning of the 'subject' field in the e-mail.
- Name or corporate name, complete domicile and e-mail address of the sender (including the complete name of a contact person).
- The inclusion of an e-mail address to which the receiver can send an e-mail in order to opt-out of receiving more unsolicited commercial e-mails, or another internet-based mechanism that enables opt-out.

A commercial e-mail is not considered unsolicited if it has been previously requested by the recipient (expressly and in writing) or if there is a prior contractual relationship with the recipient as long as the commercial communications sent refer to goods and services of the contracting company that are similar to goods or services contracted for.

Peru also offers a do not contact list. The Register of the Institute for Defence of Competition and Protection of the Intellectual Property (INDECOPI) called “Thanks ... do not insist”, is intended for users that do not want to receive calls, text messages or e-mails. Users can register five phone numbers (land lines or mobile phones) and e-mail addresses at the INDECOPI webpage. Companies that use call centres, telephone calls systems, or send bulk text messages or e-mails, as well as those that provide telemarketing services must exclude from their lists all the numbers and addresses already registered at the INDECOPI webpage.

The 'do not contact list' registered before INDECOPI does not apply to communications that have been previously requested by the recipient (expressly and in writing) or if there is a prior contractual relationship with the recipient, as long as the commercial communications sent refer to goods and services of the contracting company that are similar to goods or services contracted for.

The General Agency on Data Protection has recently interpreted that, in order to send a commercial e-mail to someone who is not protected by the “do not contact list”, the sender must comply with the requirements of the Anti Spam Law or, alternatively, seek consent from the recipient.

ONLINE PRIVACY

The PDPL does not expressly regulate On-Line privacy, including cookies and location data. However, the PDPL will apply if personal data is collected and processed using these mechanisms.

KEY CONTACTS

Rodrigo, Elias & Medrano Abogados
www.estudiorodrigo.com

Jean Paul Chabaneix
Senior Partner
T +511 6191900
JPChabaneix@estudiorodrigo.com

Ximena Aramburu
Associate
T +511 6191900
Fbaldeon@estudiorodrigo.com

Francisco Baldeón
Associate
T +511 6191900
Fbaldeon@estudiorodrigo.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

PHILIPPINES

Last modified 27 January 2016

LAW IN PHILIPPINES

The Philippines recently enacted the Data Privacy Act of 2012 (the 'Act') or Republic Act No. 10173, which took effect on 8 September 2012.

DEFINITIONS

Definition of personal data

Personal Information is defined in the Act as 'any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.'

The Act, in addition to defining 'Personal Information' that is covered by the law, also expressly excludes certain information from its coverage. These are:

- information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
    - the fact that the individual is or was an officer or employee of the government institution
    - the title, business address and office telephone number of the individual
    - the classification, salary range and responsibilities of the position held by the individual, and
    - the name of the individual on a document prepared by the individual in the course of employment with the government.
- information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services
- information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit
- personal information processed for journalistic, artistic, literary or research purposes
- information necessary in order to carry out the functions of a public authority which includes the processing of

personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act ('CISA').

- information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Philipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws, and

- personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

Definition of sensitive personal data

Sensitive Personal Information is defined in the Act as personal information:

- about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations

- about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings

- issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licences or its denials, suspension or revocation, and tax returns, and

- specifically established by an executive order or an act of Congress to be kept classified.

NATIONAL DATA PROTECTION AUTHORITY

The Act provides for the creation of a National Privacy Commission. As of 21 January 2015, the National Privacy Commission has not been constituted.

REGISTRATION

There is no system of mandatory registration provided in the Act.

DATA PROTECTION OFFICERS

The Personal Information Controller of an organisation must appoint a person or persons who shall be accountable for the organisation's compliance with the Act, and the identity of such person or persons must be disclosed to the data subjects upon the latter's request. The Act does not specifically provide for the citizenship and residency of the data protection officer. The Act likewise does not specifically provide for penalties relating to the incorrect appointment of data protection officers.

COLLECTION & PROCESSING

The collection and processing of Personal Information must comply with the general principle that Personal Information must be:

- collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate

purposes only

- processed fairly and lawfully
- accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted
- adequate and not excessive in relation to the purposes for which they are collected and processed
- retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defence of legal claims, or for legitimate business purposes, or as provided by law, and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed:
    - provided that personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods, and
    - provided, further, that adequate safeguards are guaranteed by said laws authorising their processing.

In addition, the processing of personal information must meet the following criteria, otherwise, such processing becomes prohibited:

- the data subject has given his or her consent
- the processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract
- the processing is necessary for compliance with a legal obligation to which the personal information controller is subject
- the processing is necessary to protect vitally important interests of the data subject, including life and health
- the processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate, or
- the processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

The processing of sensitive personal information is prohibited, except in the following cases:

- the data subject has given his or her specific consent prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing
- the processing is provided for by existing laws and regulations, provided that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information, and the consent of the data subjects is not required by law or regulation permitting the processing of the sensitive personal information or the privileged information
- the processing is necessary to protect the life and health of the data subject or another person, and the data

subject is not legally or physically able to express his or her consent prior to the processing

- the processing is necessary to achieve the lawful and non-commercial objectives of public organisations and their associations, provided:
    - such processing is only confined and related to the bona fide members of these organisations or their associations
    - the sensitive personal data are not transferred to third parties, and
    - the consent of the data subject was obtained prior to processing
- the processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured, or
- the processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

TRANSFER

The transfer of Personal Information is permitted without any restrictions or prerequisites, but the Personal Information Controller remains responsible for personal information under its control or custody that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. The transfer, however, of sensitive personal information to third parties is prohibited.

SECURITY

The personal information controller must implement reasonable and appropriate organisational, physical and technical measures to protect personal information against any type of accidental or unlawful destruction, such as from accidental loss, unlawful access, fraudulent misuse, unlawful destruction, alteration, contamination and disclosure, as well as against any other unlawful processing.

The determination of the appropriate level of security must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organisation and complexity of its operations, current data privacy best practices and the cost of security implementation.

In addition, the security measures to be implemented must include the following, which are subject to guidelines that the National Privacy Commission may issue:

- safeguards to protect its computer network against accidental, unlawful or unauthorised usage or interference with or hindering of their functioning or availability
- a security policy with respect to the processing of personal information
- a process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach, and
- regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

The personal information controller is obligated to ensure that third parties processing personal information on its behalf shall implement the security measures required by the Act.

The obligation to maintain strict confidentiality of personal information that are not intended for public disclosure extends to the employees, agents or representatives of a personal information controller who are involved in the processing of such personal information.

BREACH NOTIFICATION

The Personal Information Controller is required to promptly notify the National Privacy Commission and the affected data subjects when it has reasonable belief that sensitive personal information or other information has been acquired by an unauthorised person, and that:

- such personal information may, under the circumstances, be used to enable identity fraud, and
- the Personal Information Controller or the National Privacy Commission believes that such unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach.

Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. The National Privacy Commission may also authorise postponement of notification where such notification may hinder the progress of a criminal investigation related to a serious breach.

Notification is not required if the National Privacy Commission determines:

- that notification is unwarranted after taking into account compliance by the Personal Information Controller with the Act and the existence of good faith in the acquisition of personal information, or
- in the reasonable judgment of the National Privacy Commission, such notification would not be in the public interest or in the interests of the affected data subjects.

ENFORCEMENT

The National Privacy Commission is responsible for ensuring compliance of the Personal Information Controller with the Act. It has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicise any such report. Additionally, the National Privacy Commission can issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest.

The National Privacy Commission, however, cannot prosecute violators for breach of the Act for which criminal penalties can be imposed. The Department of Justice is tasked with the prosecution for violations of the Act that are punishable with criminal sanctions.

The following actions are punishable by the Act with imprisonment in varying duration plus a monetary penalty:

- processing of personal information or sensitive personal information:
    - without the consent of the data subject or without being authorised by the Act or any existing law, or
    - for purposes not authorised by the data subject or otherwise authorised under the Act or under existing laws
- providing access to personal information or sensitive personal information due to negligence and without being

authorised under this Act or any existing law

- knowingly or negligently disposing, discarding or abandoning the personal information or sensitive personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection

- knowingly and unlawfully, or violating data confidentiality and security data systems, breaking in any way into any system where personal and sensitive personal information is stored

- concealing the fact of such security breach, whether intentionally or by omission, after having knowledge of a security breach and of the obligation to notify the National Privacy Commission pursuant to Section 20(f) of the Act

- disclosing by any personal information controller or personal information processor or any of its officials, employees or agents, to a third party personal information or sensitive personal information without the consent of the data subject and without malice or bad faith, and

- disclosing, with malice or in bad faith, by any personal information controller or personal information processor or any of its officials, employees or agents of unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her.

ELECTRONIC MARKETING

In 2008, the Department of Trade and Industry, the Department of Health, and the Department of Agriculture issued a joint administrative order implementing the Consumer Act of the Philippines (Republic Act No. 7394) and the E-Commerce Act (Republic Act No. 8792). The Joint DTI-DOH-DA Administrative Order No. 01 (the 'Administrative Order') provides rules and regulations protecting consumers during online transactions, particularly on the purchase of products and services. It covers both local and foreign-based retailers and sellers engaged in e-commerce.

The Administrative Order particularly requires retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce with consumers to refrain from engaging in any false, deceptive and misleading advertisement prohibited under the provisions of the Consumer Act of the Philippines.

In line with the Administrative Order's provision on fair marketing and advertising practices, retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce are mandated to provide:

- fair, accurate, clear and easily accessible information describing the products or services offered for sale such as the nature, quality and quantity thereof

- fair, accurate, clear and easily accessible information sufficient to enable consumers to make an informed decision whether or not to enter into the transaction, and

- such information that allows consumers to maintain an adequate record of the information about the products and services offered for sale

Section 4(c)(3) of the CPA was struck down by the Supreme Court for violating the constitutionally guaranteed freedom of expression.

ONLINE PRIVACY

The CPA is the first law in the Philippines which specifically criminalises computer crimes. The law aims to address legal issues concerning online interactions. The CPA does not define nor does it particularly refer to online privacy, however,

it penalises acts that violate an individual's rights to online privacy, particularly those interferences against the confidentiality, integrity and availability of computer data and systems.

All data to be collected or seized or disclosed will require a court warrant. The court warrant shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce showing that there are:

- reasonable grounds to believe that any of the crimes penalised by the CPA has been committed, or is being committed, or is about to be committed
- reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes, and
- no other means readily available for obtaining such evidence.

The integrity of traffic data shall be preserved for a minimum period of six months from the date of the transaction.

Courts may issue a warrant for the disclosure of traffic data if such disclosure is necessary and relevant for the purposes of investigation in relation to a valid complaint officially docketed.

No law in this jurisdiction currently deals with the subject of Location Data or the regulation of the use of Cookies.

KEY CONTACTS

Romulo Mabanta Buenaventura Sayoc & De Los Angeles
www.romulo.com/

Eileen Rosario Cordero-Batac
Partner
T +63 2 555 9555
eileen.batac@romulo.com

Catherine O. King Kay
Associate
T +63 2 555 9555
catherine.kingkay@romulo.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

POLAND

Last modified 28 January 2016

LAW IN POLAND

As a member of European Union, Poland implemented EU Data Protection Directive 95/46/ EC in the Personal Data Protection Act of 29 August 1997 (consolidated text Journal of laws of 2015, item 2135 as amended, hereinafter referred to as the "PDPA"). The implementation was introduced by the Amendment of Certain Laws in Connection with Membership of the Republic of Poland in the European Union of 24 August 2007 (Journal of laws of 2007, No 176, item 1238)

DEFINITIONS

Definition of personal data

The PDPA states that personal data shall mean any information relating to an identified or identifiable natural person. An identifiable person is the 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/her physical, physiological, mental, economic, cultural or social identity.

A piece of information shall not be regarded as identifying where the identification requires an unreasonable amount of time, cost and manpower.

Definition of sensitive personal data

Pursuant to the PDPA sensitive personal data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade union membership, as well as personal 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.

NATIONAL DATA PROTECTION AUTHORITY

General Inspector of Personal Data Protection
(*Generalny Inspektor Ochrony Danych Osobowych*)

Stawki 2
00-193 Warsaw, Poland

T (22) 860 70 86 or (22) 860 70 70 (hotline)
F (22) 860 70 86

kancelaria@giodo.gov.pl

REGISTRATION

As a general rule, data controllers who process personal data must notify the General Inspector about the data filing system containing such data. The General Inspector keeps a register of data controllers and data filing systems, which is available to the public.

The obligation to register data filing systems does not apply to the data controllers of data which:

- include confidential information
- were collected as a result of inquiry procedures conducted by officers of 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 the National Criminal Register
- are processed by the Inspector General of Financial Information
- are processed by relevant bodies for the purpose of Poland's participation in the Schengen Information System and Visa Information System
- are processed by relevant bodies on the grounds of laws which regulate the exchange of information with law enforcement agencies of EU Member States
- 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 the 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 health care services, notarial or legal advice, patent agent, tax consultant or auditor services
- are created on the basis of electoral regulations concerning the Lower Chamber of the Polish Parliament, the Senate, the European Parliament, communal councils, district councils and provincial councils, the President of the Republic of Poland, the head of a commune, the mayor or president of a city, and acts on national referendums and municipal referendums
- 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 in the preparation of a thesis required to graduate from a university or be awarded a degree
- are processed with regard to minor, everyday affairs, or
- are processed in data files that are not generated with the use of IT systems, with the exception of sensitive personal data.

In addition, the data controller is exempted from the obligation to register data files if it processed non-sensitive personal data and it appointed a data protection officer (Administrator Bezpieczeństwa Informacji - ABI). The appointment of a data protection officer should be notified to the General Inspector, who keeps a register of data protection officers. The

notification procedure is formalised.

The data controller may start the processing of data in the data filing system after notification of the system to the General Inspector, unless the controller is exempted from this obligation. Nevertheless, the data controller of sensitive data may start the processing of these data in the data filing system after registration of the file, unless the data controller is exempted from the obligation to submit the system for registration.

The notification should include, in particular, the following information:

- the identity of the data controller and any data processors
- the legal grounds for data processing
- the purpose of the processing
- a description of the categories of the data subjects
- the scope of processing of the data
- the means of data collection and disclosure
- a description of the technical and organisational measures undertaken in order to comply with the goals defined in the PDPA, and
- information relating to the possible data transfer to a third country.

DATA PROTECTION OFFICERS

A data controller is not obliged to appoint a data protection officer. However, if a data protection officer is appointed and registered with the General Inspector, the data controller is not obliged to register the data filing system with the General Inspector if the data processed are non-sensitive. The data protection officer is not explicitly required to be a citizen or resident of Poland, but he/she must have full civil rights, necessary knowledge on data protection subject and a clean criminal record.

Incorrect appointment (e.g., appointing a person not meeting the legal requirements) of the data protection officer may result in removal from the registry by decision of the General Inspector. Additionally, if it results in violation of the provisions of the PDPA, it may lead to the administrative responsibility of the data controller and the entrepreneur - by decision of the General Inspector.

The scope of the data protection officer's responsibilities is specified in detail. In particular, the data protection officer is obliged to keep an open register of data files, carry out inspections as to compliance with the provisions of the PDPA and prepare reports based on such inspections. The data protection officer is also obliged to carry out an inspection at the request of the General Inspector.

The data controller is obliged to ensure the organisational autonomy of the data protection officer since the data protection officer should report directly to the head of the organisational unit of the data controller (which is usually the management board). The procedure for the notification of the data protection officer's appointment to the General Inspector is formalised. If the data controller decides not to appoint a data protection officer, the duties of the data protection officer, except for the obligation to prepare reports, are performed by the data controller. In such a situation, the data controller does not keep a register of data files, but it is obliged to register the data files with the General Inspector, unless the PDPA provides for an exemption from this obligation.

COLLECTION & PROCESSING

The processing of data is permitted only if:

- the data subject has given his/her consent, unless the processing consists in 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.

Where sensitive data is processed, one of the following conditions must be met:

- the data subject has given his/her written consent, unless the processing consists of the erasure of personal data;
- the specific provisions of other statutes provide for the processing of such data without the data subject's consent and provide for adequate safeguards;
- 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/her consent until he establishes who is the guardian or curator;
- processing is necessary for the purposes of carrying out the statutory objectives of churches and other religious unions, associations, foundations, and other non profit organisations or institutions with a political, scientific, religious, philosophical, or trade union aim provided that the processing relates solely to the members of those organisations or institutions or to the persons who have a regular contact with them in connection with their activity and subject to providing appropriate safeguards of the processed data;
- processing relates to the data necessary to pursue a legal claim
- processing is necessary for the purposes of carrying out the obligations of the controller with regard to employment of his/her employees and other persons, and the scope of processing is provided by the law;
- processing is required for the purposes of preventive medicine, the provision of care or treatment, where the data are processed by a health professional subject involved in treatment, other health care services, or the management of health care services and subject to providing appropriate safeguards;
- the processing relates to those data which were made publicly available by the data subject;
- it is necessary to conduct scientific research including reparations of a thesis required for graduating from university or receiving a degree; any results of scientific researches shall not be published in a way which allows identifying data subjects; and
- data processing is conducted by a party to exercise the rights and duties resulting from decisions issued in court or administrative proceedings.

The data controller is obliged to provide a data subject with information including: the identity of the data controller, the purpose of data collection, 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/her data and the right to rectify these data, whether the replies to the

questions are obligatory or voluntary, and in case of existence of the obligation about its legal basis. Further information is required if personal data has not been obtained from a data subject.

TRANSFER

The transfer of personal data to a third country (i.e. a country outside the European Economic Area) may take place only if the country of destination ensures an adequate level of data protection.

The adequate level of protection of personal data is evaluated taking into account all the circumstances surrounding the data transfer, in particular taking into account the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and country of final destination of the data, the laws applicable in the third country, safety measures used in this country and business conduct.

Nevertheless, the data controller may transfer the personal data to a third country provided that:

1. the data subject has given his/her written consent
2. 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
3. the transfer is necessary for the performance of a contract concluded in the interests of the data subject between the controller and another subject
4. the transfer is necessary or required by reasons of public interest or for the establishment of legal claims
5. the transfer is necessary in order to protect the vital interests of the data subject, or
6. the transfer relates to data which are publicly available.

In cases other than those referred to above, the transfer of personal data to a third country which does not ensure at least the same level of personal data protection as that in force in Poland may take place only subject to the prior consent of the General Inspector, provided that the data controller ensures adequate safeguards with respect to the protection of the privacy, rights and freedoms of the data subject. The prior consent of the General Inspector is not required if:

- the data controller executes an agreement with the data importer based on the Standard Contractual Clauses approved by the European Commission, or
- the data controller implements 'Binding Corporate Rules' which have been approved by the General Inspector.

For the transfer of data to United States, compliance with US/EU Safe Harbor principles satisfies the requirement of the PDPA and the consent of the General Inspector is not required.

The transfer of personal data is also allowed if it is required by legal provisions or by the provisions of any ratified international agreement which guarantees an adequate level of personal data protection.

Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US.

SECURITY

The data controller is obliged to implement technical and organisational measures to protect the personal data being processed, appropriate to the risks and category of data being protected, and to protect data against unauthorised

disclosure, takeover by an unauthorised person, processing which violates the PDPA, any change, loss, damage or destruction, and in particular the data controller should:

- keep the documentation describing the way of data processing and security measures;
- appoint a data protection officer who supervises the compliance with security measures (however, as mentioned above, if a data protection officer is not appointed, the given tasks in this regard should be performed by the data controller);
- ensure supervision over the following: what data is entered into the filing system, when, and by whom, and to whom they are transferred; and
- grant authorisation to persons who are allowed to carry out the processing of data and keep a register of those authorised persons, including the following information: full name of the authorised person, date of granting and expiry of the authorisation to access personal data, as well as the scope thereof, and an identifier if the data are processed in a computer system.

There are three levels of security measures depending on the category of data: "basic", "medium" and "high". In the event no sensitive data is processed and none of the devices of the IT system used for data processing is connected with the public network (i.e. the Internet) security measures should be applied at a basic level. If the data controller processes sensitive data, security measures should be applied at least at the medium level. If at least one device of the IT system used for data processing is connected to the public network, security measures should be applied on the high level.

BREACH NOTIFICATION

There is no requirement in the PDPA to report data security breaches or losses to the General Inspector or to data subjects. However, pursuant to the Telecommunications Act the provider of telecommunications services is obliged to immediately, but not later than within 3 days from learning about a data breach, inform the General Inspector about such a data breach. In the event that the breach could have a negative impact on the rights of a subscriber or end user being an individual, the service provider should immediately, but not later than within 3 days from learning about the data breach, inform the subscriber or end - user about this breach. In addition, pursuant to the Polish Code on Criminal Procedure there is a civic duty to inform the state prosecutor or Police in case of the commission of an offence prosecuted ex officio. Non compliance with the PDPA is an offence.

ENFORCEMENT

In Poland the General Inspector is responsible for the enforcement of the PDPA.

Where there is a breach of the provisions on personal data protection, the General Inspector ex officio or upon a motion of a person concerned, by means of an administrative decision, may issue orders to restore the proper legal state. Failure to comply with the decision is subject to fines up to approximately EUR 50,000.

Furthermore, non compliance with the PDPA may be a criminal offence. A person who is liable (usually a member of a management board of the company which is a data controller) may be subject to a fine (from approximately EUR 25 to approximately EUR 270,000), a partial restriction of freedom or a prison sentence of up to three years.

ELECTRONIC MARKETING

Electronic marketing activities are subject to the regulations of the PDPA, the Act of 18 July 2002 on Providing Services by Electronic Means (Journal of Laws of 2013, item 1422 as amended ('PSEM') and the Telecommunications Act of 16 July 2004 (Journal of Laws of 2014, item 243 as amended ('Telecommunications Act').

The PDPA applies to electronic marketing activities as such activities will involve processing of personal data, eg an e-mail address is likely to be considered personal data for the purposes of the PDPA. The PDPA lays down the grounds

for processing of personal data for marketing purposes. According to the PDPA the data controller may process personal data if processing is necessary for the purpose of legitimate interests pursued by the data controllers provided that the processing does not violate the rights and freedoms of the data subject.

The legitimate interests includes direct marketing of own products or services provided by the data controller. Therefore, if marketing activities relate only to products and services owned by the data controller, consent for such processing is not required. The data subject may always object to such processing. Nevertheless, if marketing activities relate to products and services not owned by the data controller, prior consent for such processing is necessary. In each case the data subject should be informed about processing of his/her personal data for marketing purposes.

Apart from consent for processing of personal data (if such consent is required), the PSEM imposes an obligation to obtain a separate consent for sending commercial information by electronic means, (eg emails and SMS) to the specified recipient who is an individual. Therefore, a service provider is obliged to obtain the relevant consent before sending the commercial information (via email or SMS) to a natural person. The consent is also required to send marketing information to a specific employee's business email address (such as name.surname@company.com). On the other hand, it is permitted to send such information without prior consent to recipients who are legal persons to a general email addresses (such as office@company.com). The consent should not be presumed to be or be part of another statement of will and may be withdrawn at any time. Sending commercial information without consent is considered to be unfair competition practice. A service provider should be able to provide evidence that it has obtained consent.

The amendment to the Telecommunications Act which implements Directive 2002/65/EC and Directive 2002/58/EC came into force on 25 December 2014. The amended regulation prohibits the use of final telecommunications devices (such as fixedline telephones, cell phones, faxes, computers, etc) and automated calling systems for direct marketing, unless a subscriber (understood as an entity who is a party to an agreement for the provision of telecommunications services concluded with a provider of publicly available telecommunications services) or end user (ie an entity using or requesting a publicly available telecommunications service to satisfy its own needs) has given prior consent to this. The regulation in the Telecommunications Act concerns all subscribers and end users (ie not only natural persons but also the legal persons).

Therefore, pursuant to the Telecommunications Act, using end telecommunications devices (for instance, to present a marketing offer during a telephone call) or automated calling systems for direct marketing requires the obtaining of another consent decision from the recipient (subscriber or end user). In practice, the relationship between the abovementioned regulations (especially between the provisions of PSEM and the Telecommunications Act) and the scope of particular consent decisions that should be obtained by service providers is not perfectly clear in this regard. However, it seems that, generally, the consent for the use of end telecommunications devices and automated calling systems for direct marketing should be obtained separately from the consent for the processing of personal data (if required) and for the sending of commercial information by electronic means.

The consent of the subscriber or the end user:

- may not be presumed or implied by a declaration of will of a different content;
- may be expressed by electronic means, provided that it is recorded and confirmed by the user; and
- may be cancelled at any time, in a simple manner and free of charge.

Enforcement and sanctions

Failing to fulfill the obligations to obtain consent for using end telecommunications devices and automated calling systems for direct marketing is subject to a financial penalty up to 3% of the revenues of the fined company for the past calendar year. The penalty is imposed by the President of the Office of Electronic Communication (hereinafter referred to as the 'President of OEC'). In addition, the President of OEC may impose a financial penalty on a person in charge of the company up to 300% of his/her monthly remuneration.

Sending marketing information by electronic means without consent is subject to criminal liability (a fine) and is considered to be an act of unfair competition.

The sanctions relating to PDPA set out in the Enforcement section above will apply accordingly.

ONLINE PRIVACY

The Telecommunications Act regulates the collection of transmission and location data and the use of cookies (and similar technologies). The amendment to the Telecommunications Act which implements Directive 2009/136/EC and Directive 2009/140/EC came into force on 21 January 2013, with the exception of the new provisions regarding cookies, which came into force by 22 March 2013.

Transmission data

The processing of transmission data (understood as data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data, which should be understood as any data processed in a telecommunications network or as a part of telecommunications services indicating geographic location of terminal equipment of a user of publicly available telecommunications services) for marketing telecommunications services or for providing value-added services is permitted if the user (i.e. subscriber or end user) gives his/her consent.

Data about location

In order to use data about location (understood as location data beyond the data necessary for message transmission or billing), a provider of publicly available telecommunications services has to:

- obtain the consent of the user to process data about location concerning this user, which may be withdrawn for a given period or in relation to a given call; or
- perform the anonymisation of this data.

A provider of publicly available telecommunications services is obliged to inform the user, prior to receiving its consent, with regard to the type of data about location which is to be processed, with regard to the purpose and time of its processing, and whether this data is to be passed on to another entity in order to provide a value-added service.

Data about location may be processed only where this is necessary to provide value-added services.

Cookies

The use and storage of cookies and similar technologies requires:

- providing clear and comprehensive information to the user;
- obtaining the consent of the user; and
- that stored information or gaining access to this stored information does not cause configuration changes in the telecommunications device of the user or the software installed on this device.

The user may grant consent by using the settings of the software installed in the final telecommunications device used by him/her or by the service configuration.

According to the explanations of the Ministry of Administration and Digitalisation, which has prepared the amendment to the Telecommunications Act, consent can be inferred by a user's actions, eg the user is given clear and relevant information about the cookies that are used and on that basis gives his/her consent by changing browser settings.

Consent is not required if storage or gaining access to cookies is necessary for:

- transmitting a message using a public telecommunications network; or
- delivering a service rendered electronically, as required by the user.

Enforcement and sanctions

A company that processes transmission data contrary to the Telecommunications Act or fails to fulfill obligations to obtain consent for processing data about location or storing and gaining access to cookies is subject to a financial penalty up to 3% of the company's revenues for the past calendar year. The penalty is imposed by the President of OEC. In addition, the President of OEC may impose a financial penalty on a person in charge of the company up to 300% of his/her monthly remuneration.

The sanctions relating to PDPA set out in the Enforcement section above will apply accordingly.

KEY CONTACTS

Justyna Wilczyńska-Baraniak
Counsel, Head of IPT
T +48 22 540 74 15
justyna.wilczynska-baraniak@dlapiper.com

Damian Karwala
Senior Associate
T +48 22 540 74 16
damian.karwala@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

PORTUGAL

Last modified 12 January 2016

LAW IN PORTUGAL

Portuguese Data Protection Law – Law nº. 67/98, of October 26th – was enacted pursuant to Directive 95/46/EC.

DEFINITIONS

Definition of personal data

The Portuguese Data Protection Law defines 'personal data' as any given information, in any format, including sound and image, related to a specific or an identifiable natural person ('data subject') An identifiable person is one who can be identified, directly or indirectly, namely by reference to a specific number or to one or more elements concerning his/her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Article 7 of the Data Protection Law defines 'sensitive personal data' as any personal data revealing one's philosophical or political beliefs, political affiliations or trade union membership, religion, private life and racial or ethnic origin and also data concerning health or sex life, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

Comissão Nacional de Protecção de Dados
*('*National Commission for the Protection of Data' also known as 'CNPD').

Rua de São Bento n°. 148, 3°
1200-821 Lisbon

T +351 21 392 84 00
F +351 21 397 68 32

geral@cnpd.pt
www.cnpd.pt

REGISTRATION

Data controllers who process personal data shall notify the Data Protection Authority ('CNPD'), unless an exemption applies. For certain categories of data (sensitive data when permitted, data regarding illicit activities or criminal and administrative offenses or credit and solvability data) and certain specific processing, prior authorisation from CNPD is required. Any variations or changes to the processing of personal data will determine the amendment of the registration.

As for the filing requirements, CNPD has an official form that must be submitted in Portuguese with the following information:

- identity of the controller and its representative
- main software features
- the purposes of the processing
- third party entity responsible for the processing (if applicable)
- all the personal data that will be collected in each register; it is also necessary to indicate if sensitive data is to be collected as well as data concerning the suspicion of illegal activities, criminal and/or administrative offences, as well as data regarding credit and solvability
- grounds of legitimacy of the collection and a brief description of the data collection method used
- means and methods available for updating the data
- means of communication of data to other entities and their identification (if applicable), and
- any transfers of data to third countries, listing the reasons, grounds and the measures adopted in each transfer.

DATA PROTECTION OFFICERS

There is no legal requirement in Portugal for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Personal data may only be processed if the data subject has given his/her unambiguous consent or if processing is deemed necessary:

- for the execution of an agreement(s) where the data subject is party or in previous diligences for the conclusion of an agreement at the request of the data subject
- for the compliance with a legal obligation to which the controller is subject
- to protect the vital interests of the data subject if the latter is physically or legally unable of giving his/her consent
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed, or
- for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

Moreover, the data controller must provide the data subject with all the relevant processing information, which includes the identity of the data controller, the purposes of processing and the means made available to the data subject to access, amend and delete its data.

TRANSFER

For the data transfers performed within the EU/EEA countries, it is only required to notify the CNPD and data processing may commence immediately thereafter.

Transfers to non EU/EEA countries can only take place if the recipient country ensures an adequate level of protection. In any case it is mandatory to start an authorisation procedure with the CNPD and data processing can only commence once the authorisation is issued.

Exceptionally, transfers performed according to the standard Model Clauses or to Safe Harbor Certificate holders are possible. In such cases, data processing can be done immediately after filling with CNPD.*

CNPD issued on 10 November 2015 specific guidelines on IntraGroup Agreements (**"IGA"**) involving transfers of personal data to non EU/EEA countries.

CNPD considers that such transfers depend on prior authorisation from CNPD for the purposes of assessing if IGA's contain sufficient guarantees that the personal data transferred continues to benefit from the same level of protection as in the EU/EEA countries.

However, when such agreements follow EU model clauses, although such model clauses are designed for bilateral relationships, CNPD understands that there are reasons to authorise such transfers more quickly as long as the data controller declares that IGA is identical and that is in accordance with EU model clauses. Therefore, in the event that EU model clauses are respected within the scope of IGA, CNPD considers that the data controller, based on its declaration, has ensured the required level of protection (without prejudice to the possibility of CNPD verifying compliance with the Data Protection Law requirements and requesting a copy of the agreement.

* ***Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.***

Following the above mentioned Schrems Judgement CNPD issued a communication in 23 October 2015 stating that already issued authorisations for the transfer of personal data to US under Safe Harbor will be reassessed, and data controllers should suspend their data flows to the US under said authorisations.

SECURITY

The controller must implement adequate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The adequacy of such measures is assessed considering whether the measures are state of the art, the costs of implementing the measures, the nature of the data and the purpose of processing.

BREACH NOTIFICATION

Law 41/2004, of 18 August on the protection and processing of personal data in e-communications was recently amended by Law no. 46/2012, of 29 August, which transposed Directive 2009/136/EC.

Now, companies that make electronic communications services accessible to the public shall, without undue delay, notify the CNPD of a personal data breach. When the personal data breach may affect negatively the subscriber's or user's personal data, companies providing electronic communications services to the public should also, without undue delay, notify the breach to the subscriber or user so that they can take the necessary precautions.

For these purposes, a negative effect to the personal data of privacy exists when the breach may result namely in theft or identity fraud, physical harm, significant humiliation or damage to reputation.

Regardless, if a person/entity is effected by the breach of the Data Protection Law, he/she is entitled to file a claim to the CNPD and/or file a civil lawsuit to seek compensation for damages.

ENFORCEMENT

In Portugal, CNPD is responsible for the enforcement of the Data Protection Law.

Failure to comply with the obligations set forth in the Data Protection Law may be deemed as an administrative and/or criminal offence.

Article 43 determines that any person who intentionally:

- fails to notify or seek CNPD's authorisation for data processing
- provides false information in the notification or applications for authorisation for the processing of personal data
- misappropriates or uses personal data in a incompatible manner with the purpose of the collection or with the legalisation instrument
- promotes or carries out an illegal combination of personal data
- fails to comply with the obligations provided for in the Data Protection Law or in other data protection legislation when the time limit fixed by the CNPD for complying with them has expired, and
- continues to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act after notification by the CNPD not to do so, shall be subject to a penalty up to one year's imprisonment or a fine of equivalent to 120 days.

Failure to comply with any of the provisions regarding the conditions and safety of data processing and the observance of the data subjects of information and opposition rights and permanent access to the data shall be deemed as an administrative offence punishable with a fine ranging from EUR 500 and EUR 5,000.

The negligent or inadequate compliance with the obligations referred to above is also punishable by a fine which varies according to the legal nature of the infringer – individuals may be punished with a fine ranging from EUR 250 to EUR 2,500 and corporate entities may be punished with a fine ranging from EUR 1,500 to EUR 15,000.

ELECTRONIC MARKETING

The Law no. 41/2004, of 18 August on the protection and processing of personal data in e communications was recently amended by Law no. 46/2012, of 29 August, which transposed the 2009/136/EC Directive.

In relation to individuals, the sending of unrequested communications for direct marketing purposes is subject to express prior consent of the subscriber or user (that is, the 'opt in' rule applies). This includes the use of automated calling and communication that do not rely on human intervention (automatic call devices), facsimile or electronic mail, including SMS, EMS, MMS and other similar applications.

This does not apply to legal entities and accordingly unrequested direct marketing communications are allowed. Nevertheless, the 'opt out' rule applies and legal entities may refuse future communications and enroll in the non-subscribers list.

This does not prevent the supplier of a product or service that has obtained its customers' data and contacts, under the lawful terms of the Data Protection Law and in connection with the sale of a product or service, to use such data for direct marketing of its own products or services similar to those transacted, provided it ensures the customers concerned, clearly and explicitly, are given the opportunity to object to the use of such data, free of charge and in an easy manner:

- at the time of the respective collection, and
- on the occasion of each message in case the customer has not initially refused such use.

The sending of electronic mail for purposes of direct marketing disguising or concealing the identity of the entity on whose behalf such communication is made, as well as the non-indication of valid means of contact to which the recipient may send a request to stop these communications or the encouragement of recipients to visit websites that violate these provisions, is strictly forbidden. The violation of these rules consists on an administrative offence, punishable with fines ranging from Eur 5,000 to Eur 5,000,000 to legal entities.

ONLINE PRIVACY

Cookie compliance

The amended Law no. 41/2004, of 18 August now determines that the storing of information and the possibility to access information stored in a subscriber/ user's terminal is only allowed:

- if consent is based on the condition the subscriber/user has provided his or her previous consent, and
- which must be based on clear and comprehensive information, namely about the purposes of the processing.

This does not prevent technical storage or access:

- for the sole purpose of carrying out the transmission of a communication over an e-communication network, or
- if strictly necessary in order for the provider of an information society service to provide a service expressly requested by the subscriber/user.

At this point, the local regulatory Authority (CNPD) has not yet issued any guidelines regarding the definition of 'consent', namely if implied consent suffices and if the continuous use of a website results in consent. In view of Portuguese practice and the restrictive approach taken by the DPA, we are of the opinion that implied consent shall not be enough and continuous use of a website shall only be regarded as consent provided clear and evident information is given. The use of a confirmation procedure is advisable.

Traffic Data

Traffic data must be eliminated or made anonymous when no longer needed for the transmission of the communication. Prior express consent is required and may be removed at any time. It can only be done to the extent required and the time necessary for marketing electronic communications services or the provision of value added services.

Processing of traffic data is admissible when required for billing and payment of interconnections and only until the end of the period during which the bill may lawfully be challenged or payment pursued.

Complete and accurate information on the type of data being processed must be provided, as well as the purposes and duration of the processing and the possibility of disclosure to third parties for the provision of value added services. Processing should be limited to workers and employees in charge of billing or traffic management, customer inquiries, fraud detection, marketing of electronic communications services accessible to the public, or the provision of value added services, restricting to that necessary for the purposes of such activities.

Location Data

Processing of this data is allowed only if they are made anonymous or to the extent and for the duration necessary for the provision of value added services, provided it has obtained prior express consent. Prior information must also be provided.

Companies must ensure there is an option, using simple means and free of charge:

- to withdraw consent at any time, or
- temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

Non-compliance with 'Opt in' rules consists of an administrative offence, punishable with fines ranging from EUR 5,000 to EUR 5,000,000.

KEY CONTACTS

ABBC
www.abbc.pt/

Joao Costa Quinta
Partner
T 00351 21.3583620
j.quinta@abbc.pt

Margarida Leitão Nogueira
Associate
T 00351 21.3583620
m.nogueira@abbc.pt

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

ROMANIA

Last modified 27 January 2016

LAW IN ROMANIA

Even though Romania has only been a member of the European Union since 1 January 2007, the EU Data Protection Directive 95/46/EC was implemented into national legislation in November 2001 through Law no 677/2001 on the protection of individuals with regards to the processing of personal data and the free movement of such data ('Data Protection Law').

DEFINITIONS

Definition of personal data

'Personal Data' is defined under the Data Protection Law as any information referring to an identified or identifiable natural person. An identifiable person is one who can be identified either directly or indirectly by referring to a personal identification number or to one or several distinctive factors that are typical for the physical, physiological, mental, economic, cultural or social identity of the respective person.

Definition of sensitive personal data

Under the Data Protection Law, the following categories of data are deemed as sensitive personal data (data presenting special risks):

- data regarding racial or ethnical origin
- political, religious, philosophical or other similar beliefs
- affiliation to certain unions
- physical or mental health condition
- sexual life, and
- criminal or administrative offences.

Moreover, according to the template notification form issued by the National Supervisory Authority for Personal Data Processing, genetic, biometric data, national identification number, series and number of identification documents are also categorised as sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

National Authority for the Surveillance of Personal Data Processing
(in Romanian '*Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal*' or 'ANSPDCP')

28-30 Magheru Blvd
District 1, Bucharest

T +40 318 059 211
F +40 318 059 602

www.dataprotection.ro

REGISTRATION

ANSPDCP operates the national registry of data controllers which can be accessed online free of charge. Public and private entities processing certain types of personal data must notify ANSPDCP in respect of their personal data processing and obtain a data controller number.

The processing of the following types of personal data requires prior notification to ANSPDCP unless the processing is provided for by the law:

1. Personal data related to racial or ethnic origin, political, religious, philosophical beliefs or beliefs of a similar nature, trade union membership as well as data regarding the health condition and sexual life;
2. Genetic and biometrical data;
3. Geo-location data collected through electronic communication means;
4. Personal data related to offenses, criminal convictions, safety criminal measures or administrative sanctions applied to the data subject, when the processing is performed by private entities;
5. Personal data processed by electronic means, having as purpose the monitoring/evaluation of certain personality traits, such as professional competence, credibility, behaviour or other related traits;
6. Personal data processed by electronic means within record systems having as purpose the adoption of automated individual decisions regarding the creditworthiness, the economical-financial condition, deeds which trigger the disciplinary, administrative or criminal liability of natural persons, when the processing is performed by private entities;
7. Personal data of minors, processed for direct marketing activities;
8. Personal data of minors processed through internet or electronic messaging;
9. Personal data mentioned under point 1 above, processed by associations, foundations or any other non profit organizations exclusively in order to achieve the specific purpose of the organization, when the data is disclosed to third parties without the consent of the data subject.

Personal data processed through video surveillance systems, including the transfer of such data to any other state, is also subject to prior notification to the ANSPDCP. The only exception to this rule is related to personal data processed by natural persons for their personal use, including personal data obtained through the video monitoring of public areas.

Based on the standard notification form issued by ANSPDCP, the notification should include the following information:

1. the personal data that are being processed (both sensitive and non-sensitive)
2. the purpose of processing
3. the categories of targeted data subjects
4. the categories of recipients
5. information regarding the transfer outside Romania, either within the European Economic Area, to states whose level of protection has been considered as adequate by the European Commission or to other third party

countries

6. identification details of entities acting as processors on behalf of the data controller

7. the manner in which data subjects are informed regarding their rights: verbally, via a website, or through a document (in which case it must be enclosed)

8. the estimated duration of personal data processing, and

9. data security measures. In this sense, the notification must include the security policy of the data controller describing the measures undertakes in order to ensure the security of the personal data processed.

Should the controller process personal data for various purposes, a notification must be filed separately for each purpose, unless such purposes can be correlated.

The notification procedure involves two stages. The first step is to file the online application. The second step is to send by post to ANSPDCP the first page of the notification stamped and signed by the legal representative of the data controller.

Once registered in the general registry, all data controllers shall be allocated a registration number which must be indicated in all official documents of the respective entity relating to the declared purpose of processing.

DATA PROTECTION OFFICERS

Currently, there is no requirement in Romania for data controllers to appoint a data protection officer.

COLLECTION & PROCESSING

Under Data Protection Law, data controllers may collect and process personal data provided that the data subject has expressly and unequivocally consented thereto. The data subject's consent is not required under the following circumstances:

- the processing is necessary for the performance of a contractual or pre-contractual arrangement where the data subject is a party

- where the data controller needs to protect the life, physical integrity or health of the data subject or another person

- the data controller must comply with a legal obligation

- the processing is necessary for the performance of public interest measures

- the data controller has a legitimate reason for processing, provided that fundamental civil liberties of data subjects are not breached, and

- processing is performed exclusively for statistical, historical or scientific research purposes.

Where sensitive data is processed, apart from the above conditions, data controllers must comply with additional requirements, depending on the specific type of sensitive data in question.

Data controllers must ensure that the data processed are proportional in relation to the declared purpose of processing, and not excessive.

Data subjects must be thoroughly informed in respect of data processing activities. They must be provided with the

following information:

- identity of the data controller and its representative
- purpose of data processing
- recipients of personal data and transfer abroad
- rights provided by law in favour of data subjects as well as their manner of exercise, or
- the consequences of the refusal to provide personal data.

TRANSFER

Different rules shall have to be observed depending on the destination country of such personal data. Personal data transfers within the EU, the EEA (or to countries with an adequate level of protection) must only be notified to ANSPDCP, when the transfer involves the categories of personal data mentioned under section "Registration" above.

In this case, if the personal data is transferred to another EU Member State or to the EEA, no other requirement must be met other than ticking the appropriate box in the on line notification form.

If the data is transferred to a country with an adequate level of data protection, such countries shall have to be explicitly listed in the on line notification form.

Personal data transfers to third party countries outside the EU, the EEA , as well as to countries considered as not offering an adequate level of protection require an authorization from ANSPDCP.

In this case the transfer is permitted provided that the controller has obtained the data subject's consent, or has concluded a data transfer agreement with the recipient of data located in the respective third country. This contract must be submitted to ANSPDCP for its review.

For the transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of the Data Protection Law.*

As of March 2014, the ANSPDCP accepts the international transfer of data based on Binding Corporate Rules.

* ***Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.***

SECURITY

Data controllers and data processors must take appropriate technical and organizational measures to protect personal data against unauthorised or unlawful access or processing and against accidental or unlawful loss or destruction alteration, unauthorised disclosure or access to personal data, in particular where the processing involves the transmission of data over a network, and against all forms of illegal processing.

The measures taken must ensure a level of security appropriate to the nature of the data.

Minimum security measures that data controllers must comply with are described in Order no 52/2002 issued by the Romanian Ombudsman.

Data controllers must ensure that when processing data through data processors, the latter have also agreed to comply with data security obligations.

BREACH NOTIFICATION

There is not yet a mandatory requirement in the Data Protection Law to report data security breaches or losses to ANSPDCP or to data subjects.

ENFORCEMENT

ANSPDCD is entitled to investigate any breach of Data Protection Law ex officio or following a complaint filed by a prejudiced data subject. In this sense, ANSPDCP may perform an audit over data processing activities performed by data controllers.

ANSPDCP may impose administrative fines for failure to comply with the Data Protection Law, ranging from approximately EUR 112 to EUR 11,200 (the highest sanction is applied for failure to comply with security measures). The level of fines is higher in case of failure to comply with the regulations in the electronic communications sector, as further detailed below.

Under certain conditions, failure to comply with Data Protection Law may be considered as a criminal offence, in which case ANSPDCP shall contact the competent criminal authorities.

In addition to this, ANSPDCP may impose the temporary suspension of data processing activities as well as the partial or complete deletion of processed data.

ELECTRONIC MARKETING

According to Data Protection Law, data subjects must be granted the right to oppose to the processing of their personal data for direct marketing purposes (opt-out). The processing of personal data for electronic marketing purposes is further regulated under Law no. 506/2004 on the processing of personal data in the electronic communications sector implementing Directive 2002/58/CE ('Law 506/2004'). According to this law, it is forbidden to send commercial communications by using automatic systems that do not require the intervention of a human operator, by fax or electronic mail or any other similar method, except where data subjects have expressly consented in advance. It may be considered that SMS marketing falls under the same restrictions.
Moreover, cases where the data controller has directly obtained the e-mail address of a data subject upon the sale or provision of a certain service towards the latter, the controller may use the respective address for the purpose of sending electronic communications regarding similar products or services, provided that data subjects are clearly and expressly offered the possibility to oppose by way of an easily accessible and free of charge method, not only when the e-mail address is collected but also with each commercial communication received by the data subject.

ANSPDCP has not issued any specific guidelines in relation to electronic marketing.

ONLINE PRIVACY

The processing of traffic data, location data and the implementation of cookies are dealt with under Law 506/2004.

Traffic data

Traffic Data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication but no later than three years as of the date of such a communication.

However, traffic data may be retained for the purpose of marketing the services offered to data subjects, or in view of the provision of value added services, solely throughout the marketing period and provided that data subjects have previously consented to the processing of traffic data.

The processing of traffic data for billing purposes or the establishment of payment obligations for interconnection is

permitted solely for a period of three years following the due date of the respective payment obligation.

The processing of traffic data for the establishment of contractual obligations of the communication services subscribers, with payment in advance, is permitted solely for a period of three years following the date of the communication.

Data subjects may withdraw their consent at any time.

The provider of electronic communication services must inform data subjects in respect of the processed traffic data, and the duration of processing, prior to obtaining their consent.

Communication service providers and entities acting under their authority may process traffic data for:

- management of billing and traffic
- dealing with enquiries of data subjects
- prevention of fraud, or
- the provision of communication services or value added services, and is permitted only if it is necessary to fulfil such purpose.

Location data

The processing of such data is permitted in each of the following instances:

- data is rendered anonymous
- data subjects have consented to such processing for the duration necessary for the performance of value added services, or
- when the purpose of the value added service is the unidirectional and non-differentiated transmission of information towards users.

The service provider must inform the users or subscribers, prior to obtaining their consent, in respect of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent at any time.

Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, communication service providers must grant users the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Cookies

The storing of cookies on user terminals is permitted subject to the following cumulative conditions:

- users have expressly consented thereto (Law 506/2004 also provides that consent may be given by way of browser settings or other similar technologies), and
- the information requirements provided by Data Protection Law have been complied with in a clear and user-friendly manner, to include references regarding the purpose of processing of the information stored by users.

Should the service provider allow the storing of third party cookies within a users' computer terminal, they will have to be informed about the purpose of such processing and the manner in which browser settings may be adjusted in order to

refuse third party cookies.

Consent is not required where cookies are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- strictly necessary for the provision of an information service expressly requested by the subscriber or the user.

Failure to comply with the requirements of Law 506/2004 is classified as a minor offence and is sanctioned with fines ranging from EUR 1,120 to EUR 22,500. In the case of companies whose turnover exceeds approximately EUR 1,120,000, the amount of fines may reach up to 2% of the respective company's turnover.

Upon request of the courts of law, of the criminal prosecution authorities or of the authorities competent in the area of national defence and security, with the prior approval of the judge, providers of electronic communication services offered to the public and providers of electronic communication public networks shall make available, as soon as possible, but no later than 48 hours, traffic data, data regarding user terminals, as well as geo-location data.

KEY CONTACTS

Marian Dinu
Country Managing Partner
T +40 372 155 881
marian.dinu@dlapiper.com

Ana-Maria Andronic
Head of Intellectual Property and Technology
T +40 372 155 816
anamaria.andronic@dlapiper.com

Ioana Popescu
Associate
T +40 372 155 871
ioana.popescu@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

RUSSIA

Last modified 27 January 2016

LAW IN RUSSIA

Fundamental provisions of data protection law can be found in the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention) ratified by Russia in 2006 and the Russian Constitution establishing the right to privacy of each individual (articles. 23 and 24). There is also specific legislation, including the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA) and various regulatory Acts adopted to implement the DPA as well as the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees' personal data (Part XIV). Other laws may also contain data protection provisions which implement the provisions of DPA in relation to specific areas of state services or industries.

On 22 July 2014 the amendments to the DPA were adopted and came into force on 1 September 2015. The amendments require all personal data operators to store and process any personal data of Russian individuals within databases located in Russia (subject to few exceptions). The penalty for violation of this requirement is ultimately the blocking of websites involving unlawful handling of Russian personal data. A Register of Infringers of Rights of Personal Data Subjects shall be established by the *Roscomnadzor* and from there and the *Roscomnadzor* may move to block websites.

As the amendments are newly passed and not in effect yet, it is still unclear as to how this register and the website blocking would work in practice. According to clarifications of Russian regulators, storing and processing of personal data of Russian individuals outside of Russia can still be compliant with the law as long as primary (initial) storage and processing of data is done in Russia. It is still questionable whether keeping "mirror" databases in Russia and elsewhere would be deemed as compliant.

DEFINITIONS

Definition of personal data

Personal data is any information that relates directly or indirectly to the specific or defined physical person (the data subject).

Definition of sensitive personal data

Sensitive personal data is defined as special categories of personal data in Russian legislation. Such special categories include data related to race, national identity, political opinions, religious and philosophical beliefs, health state, intimacies and biometrical data.

NATIONAL DATA PROTECTION AUTHORITY

Federal Service for Supervision of Communications, Information Technologies and Mass Media or, in short, *Roscomnadzor* ('Agency')

Build. 2, 7, Kitaigorodskiy proezd
Moscow, 109074

T +7 495 987 6800
F +7 495 987 6801

http://www.rsoc.ru/

REGISTRATION

The Agency is in charge of maintaining the Registry of data controllers.

Any data controller shall notify the Agency in writing about its intention to process personal data, unless one of the following exclusions applies:

- the personal data is data about employees
- the personal data was received in connection with a contract entered into with the data subject, provided that such data is not transferred without the consent of the data subject, but used only for the performance of the contract and entering into contracts with the data subject
- the personal data is the data about members of a public or religious association and processed by such an organisation for lawful purposes in accordance with their charter documents, provided that such data is not transferred without the consent of the data subjects
- the personal data was made publicly accessible data by the data subject
- the personal data includes the surname, name and father's name only
- the personal data is necessary in order to give single access to the premises of the data controller or for other similar purposes
- the personal data is included in state automated information systems or state information systems created for the protection of state security and public order
- the personal data is processed in accordance with the law without any use of automatic devices, or
- the personal data is processed in accordance with transportation security legislation for the purposes of procurement of stable and secure transport complex and personal, community and state interests protection.

The notification letter shall contain information about:

- the full name and address of the data controller
- the purpose of the processing
- the categories of personal data processed
- the categories of the subjects whose personal data is processed
- the legal grounds for processing

- the types of processing of the personal data
- the measures of protection of personal data
- name and contact information of the physical person or legal entity responsible for personal data processing
- the commencement date
- information on occurrence of cross border transfer of personal data
- the term of processing or the conditions for termination of processing the personal data, and
- information on personal data security provision.

DATA PROTECTION OFFICERS

If the data controller is a legal entity it shall appoint a data protection officer. Such an appointment is considered to be a personal data protection measure. The data protection officer controls the data controller and its employees regarding the data protection issues, informs them of statutory requirements and organises the receiving and processing of communications from data subjects.

There are no legal restrictions as to whether the data protection officer should be a citizen or resident of the Russian Federation.

Non-appointment or improper appointment of the data protection officer is treated similarly to any other violations in observing the data protection regime by the legal entities and may be subject to general penalties and enforcement protocols as described below.

COLLECTION & PROCESSING

Data controllers may collect and process personal data where any of the following conditions are met:

- the data subject consents
- the processing is required by a federal law or under an international treaty
- the processing is required for administration of justice, execution of a court order or any other statements of public officers to be executed
- the processing is required for provision of state or municipal services
- the data controller needs to process the data to perform or conclude a contract to which the data subject is a party or beneficiary party or guarantor
- the processing is carried out for statistical or scientific purposes (except where processing is used also for advertising purposes) provided that it is impersonalised
- the processing protects the data controller's vital interests and it is impossible to have the data subject's consent
- the processing is required for execution of statutory controller's or third parties' rights or for purposes important for the community provided the data subject's rights are not in breach
- personal data that is processed was publicly made accessible by the data subject or upon his or her request

- the processing is carried out by a journalist or mass media as a part of its professional activities or for the purposes of scientific, literary or other creative activities, except if the processing would damage the data subject's rights and freedoms, or

- personal data that is processed is subject to publication or mandatory disclosure under law.

As a general rule, consent may be given in any form, but it is the data controller's obligation to provide proof that he has the data subject's consent.

In the following cases the DPA requires that the data subject's consent should be in writing:

- where the personal data is collected to be included within publicly accessible sources

- where sensitive or biometrical data is processed

- in the case of the cross border transfer of personal data, where the recipient state does not provide adequate protection of personal data, or

- where a legally binding decision is made solely on the grounds of the automated processing of personal data

Consent is deemed to have been given in writing where it is signed by hand or given in an electronic form and signed by an electronic signature.

Consent may be revoked.

Consent in writing must contain the following information:

- the identity of the data subject, his/her address and passport details and identity of the subject

- data representative (if any)

- the identity and address of the data controller or the entity that processes personal data on behalf of the data controller (if any)

- the purpose of the processing

- the list of personal data that may be collected and processed

- the types of processing that are authorised

- the term for which the consent, remains valid and way of revocation, and

- the data subject's signature.

The data controller shall ensure the confidentiality of personal data. The data controller and other persons who have access to the personal data, shall not disclose any information to a third party without the prior consent of the data subject.

TRANSFER

Prior to a transfer of personal data out of Russia, the data controller must ensure that the recipient state provides adequate protection of personal data. The fact that the recipient state ratified the Convention is sufficient grounds to deem that the state provides adequate protection of personal data for the purposes of the DPA.

Where there is no adequate protection of personal data, a cross border transfer is permitted if one of the following conditions is met:

- the data subject consents
- the transfer is provided for under an international treaty to which Russia is a signatory
- the transfer is necessary in accordance with federal laws for protection of the Constitution, state defence, security and transport system
- for the purposes of performance of a contract to which the data subject is party
- the transfer protects the data subject's vital interests where it is not possible to get the written consent of the data subject.

In addition to the above, the *Roscomnadzor* issued the Order No. 274 of 15 March 2013 '*On endorsement of the List of the Foreign States Which are Not Parties to the EC Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data'*. The Order contains the list of countries which are officially recognized by Russian authorities as 'ensuring adequate protection'. Apart of the Member States of the Convention, there are 19 so 'white-listed' states as of today.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, changing, blocking or destruction of, or damage to, personal data.

There is a recent special regulation as to the measures that the data controller should undertake to ensure security of personal data, data systems, carriers of biometrical information and technologies.

BREACH NOTIFICATION

There is no mandatory requirement to report data security breaches or losses to the Agency or to data subjects.

ENFORCEMENT

In Russia, the Agency is responsible for the enforcement of the DPA. The Agency is entitled to:

- carry out checks
- consider complaints from data subjects
- require the submission of necessary information about personal data processing by the data controller
- require the undertaking of certain actions according to the law by the data processor, including discontinuance of the processing of personal data
- file court actions
- initiate criminal cases, and
- impose administrative liability.

If the Agency becomes aware that a data controller is in violation of the law, he can serve an enforcement notice requiring the data controller to rectify the position.

A data controller can face civil, administrative or criminal liability if there is a violation of personal data law. Officers of

the data controller responsible for the offence may face disciplinary action.

Usually, in the case of violation of data protection law, the Agency will serve an enforcement notice requiring the position to be rectified and may also impose an administrative penalty and/or recommend imposing disciplinary action on the officers of the data controller who are responsible for the offence.

The maximum administrative penalty that can be imposed, as at the date of this review, is RUR (Russian Rubles) 10,000. Lately, there has been much discussion on dramatically increasing the administrative penalty.

ELECTRONIC MARKETING

Electronic marketing activities are subject to limitations set by the Russian Law on Advertising No. 38-FZ dated 13 March 2006 ('AA'), under which the distribution of advertising through telecommunications networks, in particular, through the use of telephone, facsimile and mobile telephone communications, is allowed only subject to preliminary consent of a subscriber or addressee to receive advertising.

Advertising is presumed to be distributed without preliminary consent of the subscriber or addressee unless the advertising distributor can prove that such consent was obtained. The advertising distributor is obliged immediately to stop distribution of advertising to the address of the person who made such a demand.

ONLINE PRIVACY

Russian law does not specifically regulate online privacy. The definition of personal data under the DPA is rather broad and there are views that information on number, length of visits of particular web-sites and IP address (in combination with other data allowing the user to be identified) could be considered personal data.

KEY CONTACTS

Michael Malloy
Partner
T +7 495 221 4400
michael.malloy@dlapiper.com

Pavel Arievich
Legal Director
T +7 495 221 4472
pavel.arievich@dlapiper.com

Ekaterina Golodinkina
Associate
T +7 495 221 4546
ekaterina.golodinkina@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SAUDI ARABIA

Last modified 13 February 2016

LAW IN SAUDI ARABIA

Shari'a principles (that is, Islamic principles derived from the Holy *Quran* and the *Sunnah*, the latter being the witnesses' sayings of the Prophet Mohammed), which although not codified, are the primary source of law in the KSA. In addition to *Shari'a* principles, the law in the KSA consists of secular regulations passed by government, which is secondary if it conflicts with *Shari'a* principles.

At this time, there is no specific data protection legislation in place in the KSA (although we understand that a new personal data protection law is under review by the Shura Council). *Shari'a* principles generally protect the privacy and personal data of individuals.

That said, there are certain secular regulations passed by government, which although not dedicated as a whole to data privacy/protection, contain specific provisions governing the right to privacy and data protection in certain contexts. Examples of such regulations include:

- the Basic Law of Governance (no: A/90 dated 27th Sha'ban 1412 H (corresponding to 1 March 1992)), which provides that telegraphic, postal, telephone and other means of communications shall be safeguarded. They cannot be confiscated, delayed, read or breached

- the Anti-Cyber Crime Law (8 Rabi 1, 1428 (corresponding to 26 March 2007)), which generally prohibits, amongst other things, the interception of data transmitted through an information network, the invasion of privacy through the misuse of camera-equipped mobile phones and the like, illegally accessing bank or credit data of another, or unlawful access to computers for the purpose of deleting, destroying, altering or redistributing private data

- the Telecoms Act (approved pursuant to the Royal Decree No. (M/12) dated 12/03/1422H (corresponding to 3 June 2001), which states that the privacy and confidentiality of telephone calls and information transmitted or received through public telecommunications networks shall be maintained, and disclosure, listening or recording the same is generally prohibited

- the Regulations for the Protection of Confidential Commercial Information (issued by Minister of Commerce and Industry Decision No. (3218) dated 25/03/1426H (corresponding to 4 May 2005), and as amended), which governs the protection of data considered to be "commercial secrets" under these regulations.

There may also be specific regulations applicable to certain industries, for example, in banking, the Saudi Arabian Monetary Agency (or 'SAMA') imposes a general duty of confidentiality on banks, and requires banks to provide a safe and confidential environment to ensure confidentiality and privacy of customer data. Similarly, in the healthcare sector, confidentiality requirements will apply in terms of protecting medical data of patients.

In the absence of specific regulations which apply, the courts will apply Shari'a principles, which in essence provide that an individual has a right to be compensated for losses/harm suffered as a result of the disclosure of his/her personal information and/or breach of privacy by another party. A KSA court may also, in its absolute discretion, impose other penalties on a case by case basis (for example, imprisonment and/or fines).

DEFINITIONS

Definition of personal data

In the absence of specific data protection legislation, there is no definition of "personal data".

Definition of sensitive personal data

In the absence of specific data protection legislation, there is no definition of "sensitive personal data".

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in the KSA. In respect of telecommunications services, the Communications and Information Technology Commission ('CITC') is responsible for overseeing the relevant telecoms laws and policies. SAMA is responsible for, amongst other things, overseeing commercial banks in the KSA.

REGISTRATION

There are no data protection registration requirements in the KSA.

DATA PROTECTION OFFICERS

There is no requirement in the KSA for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

There is no concept of "data controller" or "data processor" in the KSA. To ensure compliance with *Shari'a*, it is advisable to obtain data subjects' consent before processing their data.

TRANSFER

There are generally no regulations regarding transfer of data outside of the KSA, although in specific sectors, the approval of a regulatory authority may be required. We do generally recommend that consent is sought from data subjects for any processing or transfer of personal data outside of the KSA.

SECURITY

There are no specific security measures that must adopted and implemented by commercial organisations, although as a matter of best practice and to avoid unauthorised processing, disclosure, loss or theft of personal data (and therefore potential liability under *Shari'a*), it is recommended that appropriate measures (technical and organisational) are put in place to protect the personal data held.

BREACH NOTIFICATION

There are no regulations imposing a mandatory requirement to report data security breaches.

Mandatory breach notification

There are no regulations imposing a mandatory requirement to report data security breaches.

ENFORCEMENT

At this time, there is no clear designated authority responsible for the enforcement of data protection and privacy equivalent to, say, the Information Commissioner in the United Kingdom. That said, specific authorities are tasked with enforcing breaches of the other legislation that is in place (for example, please see the section above entitled 'LAW'). For example, under the Anti-Cyber Crime Law, penalties for breach can include imprisonment, fines and confiscation of equipment used in committing the relevant breach, with the Bureau of Investigation and Public Prosecution carrying out investigations, the CITC providing any technical support required, and the matter potentially being referred to the courts. Of course, the data subject can also bring a claim for compensation for harm, damage and/or losses suffered.

ELECTRONIC MARKETING

Electronic marketing is regulated by Spam Regulations issued by the CITC, which require, amongst other things, opt-in consent from the date subject to receive electronic messages.

ONLINE PRIVACY

There is no specific legislation in the KSA that regulates the use of cookies. We generally recommend that the use of cookies should be carefully and fully disclosed in a website privacy policy (which should be compliant with KSA law).

KEY CONTACTS

Mohamed Moussallati
Legal Consultant
T +966 11 201 8900
mohamed.moussallati@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SERBIA

Last modified 27 January 2016

LAW IN SERBIA

The Serbian law governing data protection issues is the Law on Protection of Personal Data ('Official Gazette of the Republic of Serbia', nos. 97/2008, 104/2009, 68/2012 and 107/2012) ('DP Law'). It became applicable on 1 January 2009 and its current version (after supplements made in the course of 2012) is in force as of 17 November 2012. At the beginning of November 2015 the Ministry of Justice published a draft of a new Law on Protection of Personal Data, which is expected to enter into legislative procedure in the beginning of 2016.

DEFINITIONS

Definition of personal data

Under the DP Law, personal data is any information on a natural person based on which the respective person is identified or identifiable (for example, name, address, e-mail address, photo etc).

NATIONAL DATA PROTECTION AUTHORITY

The Serbian data protection authority is the Commissioner for Information of Public Importance and Protection of Personal Data (*Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti*) (DPA).

It is seated in Bulevar kralja Aleksandra 15 Belgrade and its website is www.poverenik.rs.

REGISTRATION

Any person or legal entity which processes personal data in Serbia (and, based on the relevant processing, establishes a database containing personal data) has to report the relevant processing to the DPA (ie has to register the respective database and itself as the data controller). This database registration obligation generally consists of two phases – the first one is to notify the DPA of the intention to establish a database (at the latest 15 days prior to the intended database establishment date) and the second one is to report to the DPA that the respective database was created (at the latest 15 days from the date of its creation). Both phases are performed by filing prescribed forms with the DPA (both on-line through the so-called Central Register of the DPA and in hard copy via post); the respective forms contain specific data on the data controller (such as its name and address of its registered seat) and on the database itself (for example, the purpose of and legal ground for its establishment, identification of exact processing activities, types of processed data, categories of data subjects, etc.). Any subsequent change of the registered database (for example, change of the initially registered processing activities) has to be reported to the DPA as well, at the latest 15 days from the date when the particular change occurred.

DATA PROTECTION OFFICERS

There is no statutory obligation for an entity which processes personal data to have a data protection officer.

COLLECTION & PROCESSING

The collection and further processing of personal data has to be legitimate and legally grounded, meaning pursuant to the data subject's consent or as specifically provided by law.

Under the DP Law there are a few cases when a data subject's personal data may be processed without the data subject's consent (for example, one of such cases is the case when the processing is necessary for fulfilment of the data controller's statutory obligations or for preparation or realisation of an agreement concluded between a data controller and data subject) ('Exceptional Cases').

Apart from the Exceptional Cases, consent is a precondition for legitimate collection and processing of personal data, and must be informed consent, meaning that it has to contain all the information on the particular processing which is explicitly prescribed by the DP Law (for example, the data subject must be notified of the purpose of the processing, identification of exact processing activities, information on other users of the data in cases when the data controller is not its only user, information on statutory rights of the data subjects in relation to the respective processing, etc.)

Moreover, although consent is necessary, it does not automatically mean that any processing, to which a data subject has consented, will be regarded by the DPA as compliant with the DP Law. There are also other conditions which must be met under the DP Law (eg the purpose must be legitimate and clearly determined and the type and scope of processed data must be proportionate to the respective purpose).

TRANSFER

The rules on the transfer of personal data, as envisaged by the DP Law, are quite general. Under the respective rules, there are two regimes for data transfer out of Serbia depending on whether the transfer will take place with or without the DPA's prior approval. The determining factor is whether a country to which the data is to be transferred is a member state of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Relevant Convention). If a country to which the data is to be transferred has signed and ratified the Relevant Convention (such as, for example, the EU countries), the transfer from Serbia is free in the sense that it is not conditional upon prior data transfer approval of the DPA (Transfer Approval), otherwise, the Transfer Approval is necessary (such as, for example, for the transfer to the US).

In addition to the above, it should also be noted that the DPA's position regarding data transfer out of Serbia is very strict, and, thus, a procedure of obtaining the Transfer Approval (which is initiated by a written request submitted to the DPA by the Serbian entity which intends to transfer the data out of the country) is very complex, time consuming and with rather uncertain outcome.

SECURITY

There are no specific security measures prescribed by the DP Law. It is only generally prescribed that:

- personal data must be adequately protected from abuse, destruction, loss, unauthorised alterations or access, and that
- both data controllers and processors are to undertake all necessary technical, human resources and organisational measures to protect data from loss, damage, inadmissible access, modification, publication and any other abuse, as well as to provide for an obligation of keeping data confidentiality for all persons who work on data processing.

BREACH NOTIFICATION

The DP Law does not impose a duty to notify data security breach. However, it should be mentioned, for the sake of completeness, that the Law on Electronic Communications ('Official Gazette of the Republic of Serbia', nos. 44/2010,

60/2013 and and 62/2014) ('EC Law') imposes a duty on entities which are operators of public communication networks and publicly available electronic communication services ('Operators') to notify the Regulatory Agency for Electronic Communications and Postal Services (RATEL) as the competent state authority, of any breach of security and integrity of public communication networks and services, which has influenced their work significantly, and particularly on the breaches which resulted in violation of protection of personal data or privacy of the respective networks/services' users/subscribers.

Non performance of this statutory obligation can lead to offence liability and fines in range from approx. EUR 4,098.00 to EUR 16,393.00 for a legal entity, and in range from approx. EUR 410.00 to EUR 1,230.00 for a responsible person in a legal entity, plus the protective measure (prohibition to perform business activities, for a legal entity, in the duration of up to three (3) years, and prohibition to perform certain duties, for a responsible person in a legal entity, in the duration of up to one (1) year).

ENFORCEMENT

The DPA is responsible for the enforcement of the DP Law. Namely, the DPA is authorised and obliged to monitor whether the DP Law is implemented and it conducts such monitoring both ex officio and based on any complaints it receives. If it establishes, when preforming the respective monitoring, that a particular person/entity which processes personal data has acted in contravention to the statutory rules on processing, the DPA shall issue a warning to the particular data controller. It may also issue a decision by which it can:

- order the data controller to eliminate the existing irregularities within a certain period of time
- temporarily forbid particular processing, or
- order deletion of the data collected without a legal ground. The DPA's decision cannot be appealed, but an administrative dispute can be initiated against the respective decision before a competent Serbian court.

Depending on the gravity of the particular misconduct and the data controller's behaviour with respect to the same, the DPA can initiate an offence proceeding against the respective data controller before the competent court. The offences and sanctions for such are explicitly prescribed by the DP Law. The respective sanctions are monetary fines (in range from approx. EUR 410.00 to EUR 8,197.00 for a legal entity and in range from approx. EUR 41.00 to EUR 410.00 for a responsible person in a legal entity).

Moreover, criminal liability is also a possibility since a criminal offence of *Unauthorized collection of personal data* is prescribed by the Serbian Criminal Code and prescribed sanctions are a monetary fine (in an amount to be determined by the court) or imprisonment up to one (1) year (both natural persons and legal entities can be subject to the respective liability).

ELECTRONIC MARKETING

Electronic marketing is not governed by the DP Law. The rules on this subject are envisaged by the Law on Electronic Trade ('Official Gazette of the Republic of Serbia', nos. 41/2009 and 95/2013), EC Law (as defined above in the section Breach Notification), Law on Advertising ('Official Gazette of the Republic of Serbia', nos. 79/2005 and 83/2014) and Consumer Protection Law (Official Gazette of the Republic of Serbia, no. 62/2014) (Relevant Legislation).

In brief, based on the Relevant Legislation, electronic marketing is allowed if it is covered by an explicit, prior written consent of the person to whom the respective marketing is directed; additionally, recipients should always be:

- clearly informed of the identity of the sender and commercial character of the communication, whereas this information should be provided in the Serbian language prior to commencing the marketing, and
- provided with a way to opt out of future marketing messages, at any time and free of charge.

ONLINE PRIVACY

There are no specific regulations explicitly governing on-line privacy (including cookies). Accordingly, the general data protection rules, as introduced by the DP Law, are, to the extent applicable, relevant for on-line privacy as well.

On the other hand, it should be noted that the EC Law, as defined in the section Breach Notification above, introduces rules on the processing of traffic data and location data, which are obligatory for entities which are the Operators (as defined above in the section Breach Notification). Under these rules, the Operators are allowed:

- to process traffic data only as long as such data is necessary for a communication's transmission and thus, when such necessity ceases to exist, the Operators are obliged, unless exceptionally (for example, in the case when they have obtained prior consent of the data subjects for using the respective data for marketing purposes), to delete such data or to keep them but only if they make the persons to which the date relates unrecognisable, and they are allowed
- to process location data generally only if the persons to which the data relates are made unrecognisable or if they have such persons' prior consent for the purpose of providing them with value added services (but even if such consent does exist, only in the scope and for the time during which the processing is needed for the respective purpose's realisation).

Violations are subject to the fines set forth above in the Breach Notification section.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Sanja Spasenovic
Senior Associate
T Office +381 11 3094 200/ Direct T +381 11 3955 413
Sanja.Spasenovic@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SEYCHELLES

Last modified 25 January 2016

LAW IN SEYCHELLES

The Data Protection Act (the 'Act') was enacted in 2003 (Act No. 9 of 2003) with the aim of protecting the fundamental privacy rights of individuals against the use of data concerning them without their informed consent. The Act will come into operation on such date as the Minister notifies in the official Gazette.

As of May 2015, the Act has not yet come into operation.

DEFINITIONS

Definition of personal data

Personal data is defined under the Act as data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual.

Definition of sensitive personal data

The Act does not define sensitive personal data. However the Act makes provision for the Minister to modify or supplement the Data Protection Principles set out in the Act for the purpose of providing additional safeguards in relation to personal data consisting of information as to:

- the racial origin of the data subject
- his political opinions or religious or other beliefs
- his physical or mental health or his sexual life, or
- his criminal convictions.

NATIONAL DATA PROTECTION AUTHORITY

The creation of the Office of the Data Protection Commissioner is envisaged by the Act but has not yet taken place.

REGISTRATION

A person shall not hold personal data unless an entry in respect of that person as a data user, or as a data user who also carries on a computer bureau, is for the time being contained in the register of data users maintained by the Data Protection Commissioner.

The particulars to be entered into the data register are as follows:

- the name and address of the data user
- a description of the personal data to be held by it and of the purpose or purposes for which the data is to be held or used
- a description of every source from which it intends or may wish to obtain the data or the information to be contained in the data
- a description of every person to whom it intends or may wish to disclose the data (otherwise than in cases of exemptions from non-disclosure as set out in the Act)
- the name of every country outside Seychelles to which it intends or may wish directly or indirectly to transfer the data, and
- one or more addresses for the receipt of requests from data subjects for access to the data.

A person applying for registration shall state whether he wishes to be registered as a data user, as a person carrying on a computer bureau or as a data user who also carries on a computer bureau, and shall furnish the Data Protection Commissioner with the particulars required to be included in the entry to be made in pursuance of the application. Where a person intends to hold personal data for two or more purposes he may make separate applications for registration in respect of any of those purposes.

A registered person may at any time apply to the Data Protection Commissioner for the alteration of any entries relating to that person. Where the alteration would consist of the addition of a purpose for which personal data are to be held, the person may make a fresh application for registration in respect of the additional purpose.

The Data Protection Commissioner shall, as soon as practicable and in any case within the period of 6 months after receiving an application for registration or for the alteration of registered particulars, notify the applicant in writing whether his application has been accepted or refused. Where the Commissioner notifies an applicant that his application has been accepted, the notification must state the particulars which are to be entered in the register, or the alteration which is to be made, as well as the date on which the particulars were entered or the alteration was made.

No entry shall be retained in the register after the expiration of the initial period of registration except in pursuance of a renewal application made to the Data Protection Commissioner. The initial period of registration and the period for which an entry is to be retained in pursuance of a renewal application ('the renewal period') shall be a period 5 years beginning with the date on which the entry in question was made or, as the case may be, the date on which that entry would fall to be removed if the application had not been made.

The person making an application for registration or a renewal application may in his application specify as the initial period of registration or, as the case may be, as the renewal period, a period shorter than five years, being a period consisting of one or more complete years.

DATA PROTECTION OFFICERS

The Act does not contain any legal requirement to appoint a data protection officer.

COLLECTION & PROCESSING

The data protection principles set out in the Act apply to personal data held by data users. Those data protection principles are as follows:

- the information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully
- personal data shall be held only for one or more specified and lawful purposes

- personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes
- personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes
- personal data shall be accurate and, where necessary, kept up to date
- personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- an individual shall be entitled:
    - at reasonable intervals, and without undue delay or expenses to be informed by any data user whether he holds personal data of which that individual is the subject
    - to access to any such data held by a data user, and
    - where appropriate, to have such data corrected or erased.

TRANSFER

If it appears to the Data Protection Commissioner that a person registered as a data user (or as a data user who also carries on a computer bureau) intends to transfer personal data held by him to a place outside the Seychelles, the Data Protection Commissioner may, if satisfied that the transfer is likely to contravene or lead to a contravention of any data protection principle, serve that person with a transfer prohibition notice prohibiting him from transferring the data either absolutely or until he has taken such steps as are specified in the notice for protecting the interests of the data subjects in question.

In deciding whether to serve a transfer prohibition notice, the Data Protection Commissioner shall consider whether the notice is required for preventing damage or distress to any person and shall have regard to the general desirability of facilitating the free transfer of data between the Seychelles and other states.

A transfer prohibition notice shall specify the time when it is to take effect and contain a statement of the principle or principles which the Data Protection Commissioner is satisfied are contravened and his reasons for reaching that conclusion, as well as particulars of the right of appeal conferred by the Act.

The Data Protection Commissioner may cancel a transfer prohibition notice by written notification to the person on whom it was served.

No transfer prohibition notice shall prohibit the transfer of any data where the transfer of the information constituting the data is required or authorised by or under any enactment or is required by any convention or other instrument imposing an international obligation on the Seychelles.

Any person who contravenes a transfer prohibition notice shall be guilty of an offence but it shall be a defence for a person charged with an offence under this subsection to prove that he exercised all due diligence to avoid a contravention of the notice in question.

SECURITY

The Act provides that appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

BREACH NOTIFICATION

Breach notification

There is no mandatory requirement in the Act to report data security breaches or losses to the Data Protection Commissioner. However, the Act provides that the Data Protection Commissioner may consider any complaint that any of the data protection principles or any provision of this Act has been or is being contravened and shall do so if the complaint appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected.

Where the Data Protection Commissioner investigates any such complaint he shall notify the complainant of the result of his investigation and of any action which he proposes to take.

Mandatory breach notification

None contained in the Act.

ENFORCEMENT

If the Data Protection Commissioner is satisfied that a registered person has contravened or is contravening any of the data protection principles, the Data Protection Commissioner may serve that person with an enforcement notice requiring him to take such steps for complying with the principle or principles in question. In deciding whether to serve an enforcement notice the Data Protection Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.

An enforcement notice in respect of a contravention of the data protection principle concerning data accuracy may require the user to rectify or erase the data and any other data held by him containing an expression of opinion which appears to the Data Protection Commissioner to be based on the inaccurate data.

If by reason of special circumstances the Data Protection Commissioner considers that the steps required by an enforcement notice should be taken as a matter of urgency, he may include a statement to that effect in the notice.

The Data Protection Commissioner may cancel an enforcement notice by written notification to the person on whom it was served.

Any person who fails to comply with an enforcement notice shall be guilty of an offences; but it shall be a defence for the person charged with an offence under this subsection to prove that he exercised all due diligence to comply with the notice in question.

If the Data Protection Commissioner is satisfied that a registered person has contravened or is contravening any of the data protection principles, the Commissioner may serve the person with a de-registration notice stating that the Data Protection Commissioner proposes to remove from the register all or any of the particulars constituting the entry or any of the entries contained in the register in respect of that person. In deciding whether to serve a de-registration notice, the Data Protection Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress, and the Data Protection Commissioner shall not serve such a notice unless he is satisfied that compliance with the principle or principles in question cannot be adequately secured by the service of an enforcement notice.

ELECTRONIC MARKETING

Although not specifically provided for in the Act, the latter will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (for instance, an email is likely to be considered as personal data for the purposes of the Act).

ONLINE PRIVACY

The Act does not contain specific provisions in relation to online privacy.

KEY CONTACTS

Juristconsult Chambers
www.juristconsult.com

Ammar Oozeer
Barrister & Partner
T +(230) 208 5526
aoozeer@juristconsult.com

Arvin Halkhoree
Barrister
T +(230) 208 5526
ahalkhoree@juristconsult.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SINGAPORE

Last modified 27 January 2016

LAW IN SINGAPORE

Singapore enacted a new Personal Data Protection Act 2012 (No. 26 of 2012) ('Act') on 15 October 2012. The Act took effect in 3 phases:

1. Provisions relating to the formation of the Personal Data Protection Commission (the 'Commission') took effect on 2 January 2013.

2. Provisions relating to the National Do-Not-Call Registry ('DNC Registry') took effect on 2 January 2014.

3. The main data protection provisions took effect on 2 July 2014.

DEFINITIONS

Definition of personal data

'Personal data' is defined in the Act to mean 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.

Definition of sensitive personal data

There is no definition of 'sensitive personal data' in the Act.

NATIONAL DATA PROTECTION AUTHORITY

Personal Data Protection Commission

T +65 6377 3131
F +65 6273 7370

info@pdpc.gov.sg
http://www.pdpc.gov.sg/

REGISTRATION

There are no registration requirements under the Act.

DATA PROTECTION OFFICERS

Each organisation is required to appoint one or more data protection officers to be responsible for ensuring the organisation's compliance with the Act. . The data protection officer does not necessarily need to be an employee of the organisation. The contact details of at least one of these data protection officers must be published.

While there is no requirement for the data protection officer to be a citizen or resident in Singapore, the Commission suggests that the data protection officer should be readily contactable from Singapore, available during Singapore business hours and, where telephone numbers are provided, these should be Singapore telephone numbers.

Failure to appoint a data protection officer may lead to a preliminary investigation by the Commission. If an organisation or an individual fails to cooperate with the investigation, this will constitute an offence. As a result, an individual may be subject to a fine of up to S$10,000 or imprisonment for a term not exceeding 12 months, or to both. An organisation may be subject to a fine of up to S$100,000.

COLLECTION & PROCESSING

Organisations may only collect, use, or disclose personal data where:

- they obtain consent from the individual prior to the collection, use, or disclosure of the personal data
- there is deemed consent by the individual to the collection, use, or disclosure of the personal data, or
- if no consent or deemed consent is given, in specific circumstances prescribed in the Act.

An individual may at any time withdraw any consent given, or deemed given under the Act, upon giving reasonable notice to the organisation.

Further, any collection, use or disclosure of the personal data must only be for the purposes that a reasonable person would consider appropriate in the circumstances, and for purposes to which the individual has been notified of. Such notification must be made in accordance with the requirements of the Act.

TRANSFER

Transfer of personal data out of Singapore is allowed, provided that the transfer is made in accordance with the requirements of the Act to ensure that a comparable standard of protection (as set out in the Act) is accorded to personal data that is to be transferred overseas.

An organisation may apply to be exempted from any requirement prescribed under the Act in respect of any transfer of personal data out of Singapore. An exemption may be granted on such conditions as the Commission may require.

SECURITY

Organisations are obligated to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Act does not specify security measures to adopt and implement.

BREACH NOTIFICATION

Currently, there are no specific legislative requirements for data users to notify authorities regarding data protection breaches in Singapore.

Aggrieved parties may either make a complaint to the Commission, or may take out a private action in civil proceedings. The Commission may also conduct investigations on its own motion.

ENFORCEMENT

Enforcement of the Act is carried out by the Commission. The powers of the Commission include giving directions to:

- stop collection, use or disclosure of personal data in contravention of the Act
- destroy personal data collected in contravention of the Act
- provide or refuse access to or correction of personal data, and/or
- pay a financial penalty not exceeding $1 million.

These directions may be registered with the Singapore District Courts so that they may have the force and effect of an order of court.

Directions or decisions given are subject to reconsideration by the Commission, upon written application by any aggrieved party.

Directions, decisions or reconsiderations of the Commission may also be subject to appeal to a Data Protection Appeal Committee, unless the direction or decision to be appealed is the subject of an application for reconsideration, in which case such appeal would be deemed withdrawn.

Directions may only be appealed to the High Court and Court of Appeal with regard to:

- a point of law arising from a direction or decision of the Appeal Committee, or
- any direction of the Appeal Committee as to the amount of a financial penalty.

Any person who has suffered loss or damage directly as a result of a contravention of the Act is also entitled to pursue a private action in court. However, where the Commission has made a decision with regard to the said loss or damage, a right of private action will only lie after the decision has become final as a result of there being no further right of appeal. The court may grant to the plaintiff all or any of the following:

- relief by way of injunction or declaration
- damages, and/or
- such other relief as the court thinks fit.

ELECTRONIC MARKETING

The data protection principles in the Act apply to any marketing activities (including electronic marketing) which involve the collection, use or disclosure of personal data.

In addition, any organisation or person that wishes to engage in any telemarketing activities will need to comply with the "Do Not Call" provisions under the Act. Generally, a person or organisation who wishes to send marketing messages to a Singapore telephone number should first obtain the clear and unambiguous consent of the individual to the sending of the messages to such Singapore telephone number. In the absence of such consent, it would be necessary to check and ensure that the telephone number is not on a Do-Not-Call register maintained by the Commission ('DNC Register'), unless such checks are exempted under the Act. There are also other requirements, including a duty to identify the sender of the marketing message and provide clear and accurate contact information, as well as a duty not to conceal the calling line identity of any voice calls containing such marketing message. An individual may at any time apply to the Commission to add or remove his Singapore telephone number on the DNC Register.

The Act will apply to marketing messages addressed to a Singapore telephone number where:

- the sender of the marketing message is present in Singapore when the message was sent, or

- the recipient of the marketing message is present in Singapore when the message is accessed.

Electronic marketing activities are also regulated under the Spam Control Act (Cap 311A), to the extent that such activities involve the sending of unsolicited commercial communications in bulk by electronic mail or by SMS or MMS to a mobile telephone number.

ONLINE PRIVACY

Currently, there are no specific requirements relating to online privacy (including cookies and location) under the Act. Nevertheless, an organisation that wishes to engage in any online activity that involves the collection, use or disclosure of personal data will still need to comply with the general data protection obligations under the Act. For example, if an organisation intends to use cookies to collect personal data, it must obtain consent before use of any such cookies. For details of the consent required, please see the **Collection & Processing** chapter.

KEY CONTACTS

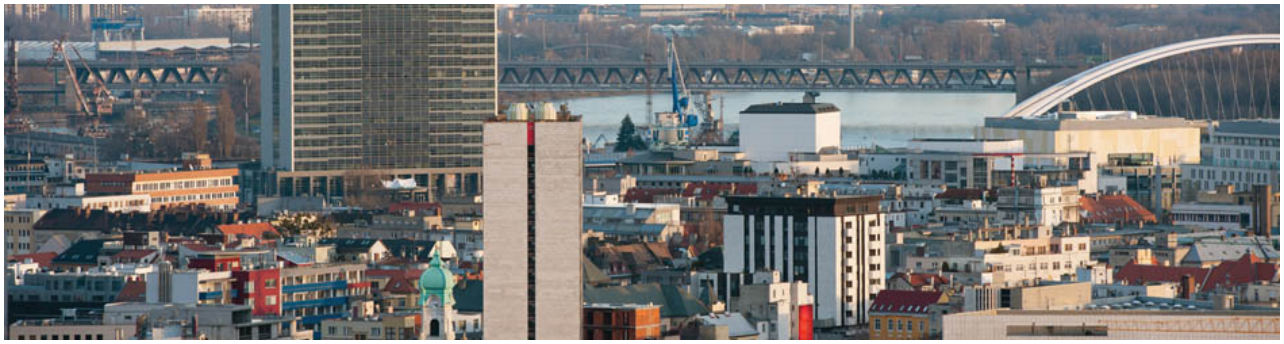
Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

Lauren Silk
Associate
T +65 6512 6053
lauren.silk@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SLOVAK REPUBLIC



Last modified 27 January 2016

LAW IN SLOVAK REPUBLIC

As a member of the European Union, Slovakia implemented the EU Data Protection Directive 95/46/EC in September 2002 with Act No. 428/2002 Coll., the Data Protection Act, as amended. In order to solve some application problems of Act No. 428/2002 Coll. resulting from the non-uniform interpretation of the definitions under this Act, the new Act No. 122/2013 Coll., the Data Protection Act ('DPA'), substituting Act No. 428/2002 Coll., has been adopted and is effective as of 1 July 2013 which has been further amended by the Act No. 84/2014 Coll. that is effective as of 15 April 2014.

DEFINITIONS

Definition of personal data

Personal data shall, for the purposes of the DPA, mean any information relating to an identified or identifiable natural person, either directly or indirectly, in particular by reference to an identifier of general application or by reference to one or more factors specific to his/her physical, physiological, psychic, mental, economic, cultural or social identity.

Definition of sensitive personal data

The DPA does not provide for a definition of sensitive personal data. However, one of the provisions of the DPA namely 'Special categories of data' refers, *inter alia*, to personal data related to race, ethnic origin, political opinions, religious belief, as well as data related to the breach of provisions of criminal or administrative law, biometrical data, or data related to the mental status of the data subject.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Office of the Slovak Republic ('Office') is: *Úrad na ochranu osobných údajov Slovenskej republiky* (Official Slovak Name)

Hraničná 12
820 07, *Bratislava* 27
Slovak Republic

The Office is responsible for overseeing the DPA in Slovakia.

REGISTRATION

The obligation to register the information system with the Office was replaced with the obligation of the data controller to notify the information systems under the conditions set out in DPA to the Office.

The obligation to notify shall apply to all information systems, in which personal data are processed by fully or partially

automated means of processing.

The information system needs to be notified before starting with the processing of the data contained therein. Notification may be carried out electronically as well as in the written form, whereas such notification is free of charge. The Office will assign an identification number to the pertinent information system, as well as issue a certificate of the fulfilment of the notification obligation to notify on the controller's request.

Despite the above, special registration shall remain applicable to the information systems that are stipulated in the DPA, inter alia, those that contain special categories of data or data processed without the data subject's consent, which is to be transferred to third countries that do not guarantee an adequate level of data protection. The Office will verify whether the data processing could infringe the rights and freedoms of data subjects and decide, within 60 days from the day of its receipt, whether or not it will permit the data processing. The said period may be prolonged by the Office, however in any case for a maximum duration of 6 months. If the Office assesses the data processing in the information system as a risk, it shall not carry out the special registration of the processing for the respective purpose. The Office will carry out the special registration for a fee of EUR 50.

DATA PROTECTION OFFICERS

The data controller is responsible for the internal supervision of protection of personal data processed pursuant to the DPA. The data controller may nominate in writing one or more data protection officers for supervising the observation of the DPA provisions in his/her/its company if he/she/it processes the personal data through authorised persons. The Office must be notified of this fact in writing by the data controller without undue delay, but no later than 30 days from such nomination.

Data protection officers may supervise the observation of the DPA provisions on the basis of his/her nomination only following the successful completion of the professional examination at the Office. The particularities of this examination are stipulated in Decree of the Office No. 165/2013 Coll.

COLLECTION & PROCESSING

Under the DPA, the data controller who intends to process personal data of the data subject must inform the data subject before obtaining the data, and notify him/her in advance of the following:

- identification data of the data controller and his/her/its representative (if appointed)
- identification data of the data processor, provided that the data controller processes personal data from the data subject through the data processor
- the purpose of the personal data processing
- list (or extent) of personal data, and
- additional information in the extent necessary for safeguarding the rights and legitimate interests of the data subject with regard to all circumstances of the processing of personal data, the particulars of which are provided in the DPA.

Personal data may be processed only by the data controller or data processor. The data processor may process personal data only to the extent and under the conditions agreed with the data controller in a written contract.

The DPA lists basic obligations of the data controller mentioned below. The data controller must, *inter alia*:

- determine unambiguously and specifically the purpose of data processing before starting the data processing; the purpose of data processing must be clear and it cannot be contrary to the Constitution of the Slovak Republic, constitutional laws, laws and international treaties binding for the Slovak Republic

- determine the conditions of the data processing in a manner so that the rights of the data subject under the DPA are not restricted
- process only accurate, complete and, where necessary, updated personal data in respect of the purpose of its processing
- destroy the personal data when the purpose of processing is terminated, and
- process personal data in accordance with public morals and act in a manner not contrary to the DPA.

Personal data may only be processed upon the consent of the data subject, unless provided otherwise for by the DPA. The consent of the data subject is not required for instance in cases when the purpose of the data processing, data subjects and the list (or extent) of the personal data is stipulated by a directly enforceable legally binding Act of the EU, an international treaty binding for the Slovak Republic, the DPA or other particular Acts. Under the DPA, the processing of special categories of data (ie sensitive information) is allowed only upon the written or other reliably verifiable consent of the data subject and following the specific conditions set forth in the DPA.

TRANSFER

Transfer to third parties within the territory of the Slovak Republic

The personal data of the data subject may be transferred from the information system to another natural person or legal entity only upon obtaining the written confirmation of the data subject's consent, if the DPA requires such consent; the person providing data in such manner may replace this written confirmation by a written declaration of the data controller stating that the data subjects gave their consent, provided that the data controller is able to prove that the written consent of the data subjects was given.

Transfer to nonEU member states (ie third countries) that offer an adequate level of data protection

If the third country guarantees an adequate level of data protection, the data may be transferred to this country if the data controller informed the data subject about the facts required to obtain the data subject's data (ie the information mentioned above in relation to data collecting by the data controller). Under the DPA, the data transfer to a country that guarantees an adequate level of protection is also allowed in cases when a notification/information to the data subject is not required.

Transfer to third countries that do not offer an adequate level of data protection

If the third country does not guarantee an adequate level of protection, the transfer of data is possible if the data controller adopts appropriate guarantees to protect:

- the privacy and fundamental rights and freedoms of natural persons (data subjects), and
- the enforcement of such rights. Such guarantees result either from standard contractual clauses under special regulations[1] or from binding internal rules of the data controller, which were approved by the supervisory authority in the field of data protection with its seat in an EU or EEA Member State.

If, in the contract on transfer of personal data to the third country which does not offer an adequate level of protection, the data controller uses the contractual clauses which are different from the contractual clauses referred to above and/or are obviously non-compliant with them, the data controller is obliged to obtain the consent of the Office for such transfer in advance.

Otherwise, the transfer of data to a third country that does not offer an adequate level of protection is possible only if the conditions mentioned below are fulfilled:

- before the actual transfer, the data subject gave a written or other reliably verifiable consent to the transfer, while

knowing that the country of final destination does not ensure an adequate level of protection

- the transfer is necessary for the execution of a contract between the data subject and the data controller or for pre contractual measures or in negotiations regarding the amendments to the contract which are initiated upon the request of the data subject
- it is necessary for entering into, or the execution of, a contract concluded by the data controller in the interest of the data subject with another entity
- it is necessary or desired under the respective law for securing an important public interest or for proving, filing or defending a legal claim resulting from an international treaty binding for the Slovak Republic or resulting from the laws
- it is necessary for the protection of vital interests of the data subject, or
- it concerns the personal data, which constitutes a part of the lists, registers or files and are kept and publicly accessible pursuant to special legislation or is available, under this legislation, to persons who prove that they are legally entitled and fulfil the conditions prescribed by law for making the data available.

Transfer to the US

For the transfer of data to the United States, compliance with the US/EU Safe Harbor principles no longer satisfies the requirements of the DPA provisions on data transfer. Following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU Safe Harbour regime is no longer regarded as a valid basis for transferring personal data to the US and further transfers taking place under the Safe Harbour decision are unlawful. However, until the appropriate solution is found with the US authorities, in order to transfer data to the US, data controllers may use the mechanisms enabling the data transfer to the countries which do not guarantee an adequate level of data protection, which are described above.

SECURITY

The data controller is responsible for the security of personal data by protecting it against damage, destruction, loss, alteration, unauthorised access and making available, providing or publishing, as well as against any other unauthorised forms of processing. For this purpose, the data controller must take reasonable technical, organisational and personal measures which correspond to the manner of processing data.

The data controller is required to prepare a security project, for certain information systems under the conditions stipulated in the DPA . Particularities of the security requirements are in detail stipulated by Decree of the Office No. 164/2013 Coll.

The data controller may nominate in writing one or more data protection officers for supervising the observation of the DPA provisions in his company if he/she/it processes the personal data through authorised persons. The data controller is required to instruct the authorised persons about the rights and obligations stipulated in the DPA before the first operation with the personal data is carried out. The data controller must establish and maintain confidentiality of the processed data even after the termination of its processing.

BREACH NOTIFICATION

Under the DPA, there is no mandatory requirement to report data security breaches or losses to the Office. However, this does not affect the ability of other public authorities to report data security infringements or losses to the Office if they suspect that such an event might have occurred.

ENFORCEMENT

The Office is responsible for the enforcement of the DPA. Upon a complaint from a data subject or another person or a report from public authorities, the Office shall commence administrative proceedings to ascertain possible breaches of obligations or conditions stipulated by the DPA and eventually shall impose a fine for these breaches. The Office may issue decisions to provide temporary relief for the data subject or to ensure due rectification depending on the nature of the breach.

The Office shall impose fines for breaches of the DPA between EUR 150 to EUR 200.000. The Office may publish a notice containing the identity of the data controller or data processor that breached the provisions of the DPA and the final decision of the Office regarding such breach, including its descriptions, and merits of the case. The Office shall also impose disciplinary fines on the data controller or the data processor in instances stipulated by the DPA.

ELECTRONIC MARKETING

Electronic marketing shall be governed by Act No. 351/2011 Coll. on Electronic Communications, as amended ('ECA').

Under the ECA, processing of the traffic data of a subscriber or user for the purposes of marketing services or purposes of ensuring the value added services by any public network or service providers is possible solely with the prior consent of the subscriber or the user.

Prior to obtaining the consent, the public network or service providers are obliged to inform the subscriber or user on:

- the type of the traffic data processed
- the purpose of the traffic data processing, and
- the duration of the data processing.

For the purposes of direct marketing, the call or use of automatic calls and communications systems without human intervention, facsimile machines, e-mail, including SMS messages to the subscriber or user, who is a natural person, is allowed solely with his/her prior consent. Such consent shall be proved. Users or subscribers are entitled to withdraw such consent at any time.

The prior consent of the recipient of a marketing e-mail shall not be required in the case of direct marketing of own similar products and services of a person, that has obtained electronic contact information of the recipient from the previous sale of its own product and/or service to such recipient and in line with the provisions of the ECA. The recipient of an e-mail shall be entitled to refuse at anytime, by simple means and free of charge such use of electronic contact information at the time of its collection and on the occasion of each message delivered in the case the recipient has not already refused such use.

Both,

- sending e-mails for the purposes of direct marketing without the determination of a valid address to which the recipient may send a request that he/she is no longer willing to receive such communication, and
- encouragement to visit a website in contradiction with a special regulation, shall be prohibited.

ONLINE PRIVACY

As regards the protection of privacy and protection of personal data processed in the electronic communications sector, the provisions of the ECA shall apply. The ECA implemented Directive 2002/58/EC (as amended by Directive 2009/136/EC).

Under the ECA, the public network or service provider is obliged to ensure technically and organisationally the confidentiality of the communications and related traffic data, which are conveyed by means of its public network and public services. In particular recording, listening, or storage of data (or other kinds of an interception or a surveillance of communications and data related thereto) by persons other than users, or without the consent of the concerned users, shall be prohibited. However, this does not prohibit the technical storage of data, which is necessary for the conveyance of communications. However, the principle of confidentiality shall still apply.

Further to this, the network or service provider ('undertaking company') shall not be held liable for the protection of the conveyed information if such information can be directly listened to or obtained at the location of the broadcasting and/or reception.

However, this ban does not apply to temporary recording and storing of messages and related traffic data if it is required:

- for the provision of value added services ordered by a subscriber or user
- to prove a request to establish, change or withdraw the service, or
- to prove the existence or validity of other legal acts, which the subscriber, user or undertaking company has made.

Under the ECA, each person that stores or gains access to the information stored in the terminal equipment of a user must be authorised for such processing by the concerned user whose consent must be based upon exact and complete information regarding the purpose of such processing of the data. In this regard, also the use of the respective setting of the web browser or other computer programme is considered (implied) consent.

Traffic Data

Traffic Data can only be processed for the purpose of the conveyance of a communication on an electronic communications network or for the invoicing thereof. The Traffic Data related to subscribers or users may not be stored without the consent of the person concerned and the undertaking company is required, after the end of a communication transmission, without delay, to destroy or make anonymous such Trafic Data, except as provided otherwise by the ECA.

If it is necessary for the invoicing of the subscribers and network interconnection payments, the undertaking company is required to store the Traffic Data until the expiration of the period during which the invoice may be legally challenged or the claim for the payment may be asserted. The undertaking company is required to provide the Traffic Data to the Office or the court in the case of a dispute between undertaking companies or between an undertaking company and a subscriber. The scope of the stored Traffic Data must be limited to the minimum necessary.

Location Data

The undertaking company may process the Location Data other than the Traffic Data which relates to the subscriber or the user of a public network or public service only if the data are made anonymous or the processing is done with user consent, and in the scope and time necessary for the provision of the value added service. The undertaking company must, prior to obtaining consent, inform the subscriber or user of the Location Data other than Traffic Data which will be processed, on the purpose and duration, and whether the data will be provided to a third party for the purpose of the provision of the value added service. The subscriber or user may revoke its consent for the processing of location data at any time.

Following the Judgment of the Court of Justice of the European Union on 8 April 2014 in the joined cases of Digital Rights Ireland (C-293/12) and Kärtner Landesregierung (C-594/12) which cancelled so called "data retention" Directive 2006/24/EC, Constitutional Court of Slovak Republic on 29 April 2015 issued a Judgement (PL. ÚS 10/2014-78) ("Judgement") upon which the Constitutional Court proclaimed the certain provisions of the ECA to be non-compliant with the provisions of the Constitution of Slovak Republic, provisions of the Charter of Fundamental Rights and Freedoms and with the provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms. Upon the Judgment, the obligation of the telecommunications operators to retain the Traffic Data and Location Data about the electronic communication of all citizens for the prescribed period (6/12 months) was abolished and removed from ECA.

KEY CONTACTS

JUDr. Dr. Michaela Stessl
Country Managing Partner
T +421 2 59202 122
michaela.stessl@dlapiper.com

Eva Skottle
Senior Associate
T +421 2 59202 111
eva.skottke@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SOUTH AFRICA

Last modified 27 January 2016

LAW IN SOUTH AFRICA

The Constitution of the Republic of South Africa guarantees the right to privacy.

Certain provisions within the Electronic Communications and Transactions Act regulate the electronic collection of personal information, although compliance with these provisions is voluntary.

The Protection of Personal Information Act ('PPI Act'), was promulgated into law on 26 November 2013, following the President's signature. The PPI Act is wide in application and will, subject to certain exclusions detailed therein, impact all persons processing personal information. The Act will commence on a date to be determined by the President by proclamation in the Government Gazette. Different dates of commencement may be determined in respect of different provisions of the PPI Act. Certain sections of the PPI Act have, on proclamation by the President of the Republic of South Africa, come into effect as of 11 April 2014. The provisions of the PPI Act which came into effect relate to the definitions section under the PPI Act and the provisions dealing with the establishment of the office of the Regulator (as well as its powers, duties and functions).

DEFINITIONS

Definition of personal data

'Personal Information' is defined broadly in the PPI Act to include information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person/legal entity and includes:

- information about a person's 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
- information relating to the education, 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.

Definition of sensitive personal data

The PPI Act provides for a separate category of information called 'Special Personal Information' which includes all information relating to a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information or criminal behaviour. The PPI Act also specifically regulates personal information of a child (who is subject to parental control in terms of the law).

Exclusions

The PPI Act provides for certain exemptions. The PPI Act will not apply to personal information processed:

- in the course of a purely personal or household activity;
- in a way in which it has been de-identified to the extent that it cannot be re-identified again;
- by or on behalf of the State with regard to national security, defence or public safety, or the prevention, investigation or proof of offences;
- for the purposes of the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;
- for exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information;
- for bona fide literary or artistic expression;
- by Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality (this option may be deleted in the final version of the PPI Act when it is promulgated);
- for purposes relating to the judicial functions of a court referred to in section 166 of the Constitution; or
- under circumstances that have been exempted from the application of the information protection principles by the Regulator (being the Information Regulator established under the PPI Act) in certain circumstances.

NATIONAL DATA PROTECTION AUTHORITY

The PPI Act introduces and provides for the establishment of an independent supervisory authority, namely the Information Protection Regulator ('Regulator') specifically established for the purpose of data protection.

The Regulator is entrusted with extensive powers and duties, including the right to establish committees, promote understanding and acceptance of the information protection conditions imposed by the PPI Act, undertake educational programmes and research, examine proposed legislation, report to Parliament, conduct audits, act as mediator, receive and investigate complaints relating to alleged violations, issue codes of conduct, assist bodies in the development of codes of conduct and publish reports.

In the performance of its functions, the Regulator is obliged to have due regard to and take account of:

- the information protection conditions
- the protection of all human rights and social interests which compete with the right to privacy (including the desirability of the free flow of information)
- international obligations accepted by South Africa, and
- developing international guidelines relevant to the protection of individual privacy.

The process to establish the Regulator is currently in progress. Parliament has received nominations for the appointment of members of the Regulator. It is anticipated that the Regulator will be appointed in the second half of

2016. Only once the Regulator has been appointed and has established an office with a budget and staff, can the process of drafting the regulations required to implement the PPI Act commence. Responsible parties (as defined below) will have 12 months from the commencement date of the PPI Act to become fully compliant with the legislation.

REGISTRATION

No registration or notification requirements for the processing of personal information as prescribed by the PPI Act other than in certain instances where a responsible party requires the prior authorisation of the Regulator with regard to certain categories of processing of personal information as detailed in section 57 of the PPI Act. A responsible party that fails to comply with the required notification procedures is guilty of an offence and may be liable to a penalty.

DATA PROTECTION OFFICERS

The PPI Act provides for the appointment of Information Protection Officers in respect of both public and private bodies. The Information Protection Officers will be responsible for encouraging compliance with the provisions of the PPI Act, dealing with any requests made to that body, and cooperating with the Regulator in respect of any investigations by the Regulator in relation to that body.

COLLECTION & PROCESSING

The PPI Act specifically imposes eight information protection conditions, namely, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. These conditions give effect to internationally accepted information protection conditions and help ensure that the PPI Act prescribes the minimum requirements for lawful processing of personal information. Responsible parties may process (which includes collecting) personal information where, inter alia:

- the information protection conditions are met
- the processing is performed in a reasonable manner that does not infringe the data subject's privacy and is for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party
- the data subject has been made aware of, inter alia, the nature of the information being collected, the identity of the responsible party and the purpose of the collection of the information
- in relation to processing, such processing is adequate, relevant and not excessive
- the data subject has consented thereto (it is to be noted that a data subject may withdraw its consent at any time), or the processing is necessary for the conclusion of a contract, complies with an obligation imposed by law, protects a legitimate interest of the data subject, or is necessary for pursuing the legitimate interests of the responsible party or a third party to whom the information is supplied
- the personal information is collected directly from the data subject (unless the information has been made public by the data subject, the data subject has consented to collection from another source, the data subject's interests would not be prejudiced by the collection, the collection is necessary per the grounds contemplated in the PPI Act, the lawful purpose of the collection would be prejudiced or compliance is not reasonably practical) the data subject will continue to have access to the personal information (subject to certain exemptions), and
- the responsible party has taken appropriate technical and organisational measures to safeguard the security of the information.

The PPI Act distinguishes between personal information and special personal information. Processing of special personal information and personal information of a child is prohibited unless such processing falls within the general authorisations prescribed under the PPI Act. The term "Special Personal Information" is discussed above. The prohibition is, however, subject to a number of exemptions.

Consent of the Data Subject

Under the PPI Act, personal information may only be processed if the data subject (or a competent person where the data subject is a child) expressly consents to the processing of the personal information, unless the exclusions with regard to consent apply. The consent of the data subject is not required where the processing of personal information:

- is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
- complies with an obligation imposed by law on the responsible party;
- protects a legitimate interest of the data subject;
- is necessary for the proper performance of a public law duty by a public body; or
- is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

Rights of Access to Data

The PPI Act allows a data subject the right to request that a responsible party correct or delete personal information that is inaccurate, irrelevant and excessive, or which the responsible party is no longer authorised to retain.

TRANSFER

The PPI Act provides that a responsible party may not transfer personal information about a data subject to a third party in a foreign jurisdiction unless:

- the recipient is subject to a law or contract which:
    - upholds principles of reasonable processing of the information that are substantially similar to the principles contained in the PPI Act, and
    - includes provisions that are substantially similar to those contained in the PPI Act relating to the further transfer of personal information from the recipient to third parties
- the data subject consents to the transfer
- the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request
- the transfer is necessary for the conclusion or performance of a contract concluded 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 consent, the data subject would be likely to give it.

SECURITY

The PPI Act significantly changes the previous position where there was no law that regulated the security of processed personal information.

Under the PPI Act, a responsible party must secure the integrity of the personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

- loss of, damage to, or unauthorised destruction of personal information, and

- unlawful access to, or processing of, personal information.

To give effect to these measures, the responsible party must take reasonable steps to:

- identify all reasonably foreseeable internal and external risks to personal information under its control
- establish and maintain appropriate safeguards against the risks identified
- regularly verify that the safeguards are effectively implemented, and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

BREACH NOTIFICATION

Under the PPI Act, where there are reasonable grounds to believe that a data subject's personal information has been accessed or acquired by an unauthorised person, the responsible party, or any third party processing personal information under the authority of the responsible party, must notify the Regulator and the data subject, unless the identity of the data subject cannot be established.

Notification to the data subject must be:

- made as soon as reasonably possible after the discovery of the breach
- sufficiently detailed, and
- in writing and communicated to the data subject by mail (to the data subject's last known physical or postal address), email to the data subject's last known email address, placement in a prominent position on the website of the responsible party, publication in the news media, or as may be directed by the Regulator.

The notification must include such detail as to allow the data subject to take protective measures.

A responsible party may be directed by the Regulator to publicise the breach where the Regulator has reasonable grounds to believe that such publicity would protect the data subject.

ENFORCEMENT

The PPI Act regulates the processing of personal information and accordingly provides for specific enforcement mechanisms.

The Regulator is responsible for the investigation and enforcement of the PPI Act.

Any person may, either orally or in writing (although oral submissions are to be converted to writing as soon as reasonably practicable), submit a complaint to the Regulator in the event of alleged interference.

The PPI Act provides that, after receipt of a complaint, the Regulator is obliged to investigate the complaint, act as a conciliator where appropriate and take further action as contemplated by the PPI Act.

In exercising its investigative powers, the Regulator may *inter alia* administer the oath, summon and enforce the appearance of persons, compel the provision of written or oral evidence under oath, receive evidence irrespective of whether such evidence is admissible in a court of law, and enter and search any premises occupied by a responsible party. Where necessary, the Regulator may apply to a judge of the High Court or a magistrate to issue a warrant to enable the Regulator to enter and search premises.

Any person who hinders, obstructs or unlawfully influences the Regulator, fails to comply with an information or enforcement notice, gives a false evidence before the Regulator on any matter after having been sworn or having made an affirmation, contravenes the conditions insofar as they relate to processing of an account number of a data subject, knowingly or recklessly, without the consent of the responsible party obtains or discloses or procures the disclosure, sells or offers to sell an account number of a data subject to another person, is guilty of an offence and liable on

conviction to a fine or imprisonment (or both) for a period of no longer than ten years, or to a fine or imprisonment for a period not exceeding12 months (or both) in respect of the other offences created by the PPI Act. Currently, the maximum fine which may be imposed is ZAR10 million although this may change once the regulations are promulgated.

Responsible parties have a right of appeal against a decision of the Regulator and a data subject has the right to institute a civil action for damages in a court against a data controller for breach of any provision of the PPI Act.

ELECTRONIC MARKETING

The Consumer Protection Act ('CPA') deals with the consumer's right to restrict unwanted direct marketing while the Electronic Communication and Transactions Act ('ECTA') regulates unsolicited electronic communications.

Under the CPA, consumers have the right to pre-emptively block any direct marketing. Any consumer who has been sent any marketing communication may demand the persons responsible for initiating the communication desist from sending any further communication to them. The ECTA has similar provisions and specifically requires that each electronic message be accompanied by an option to cancel (ie opt-out) a subscription to a mailing list and also requires the sender of the message to provide specific identifying information, including name and contact information.

Under the PPI Act, data subjects have certain rights with respect to unsolicited electronic communications (i.e. direct marketing by means of automatic calling machines, facsimile machines, SMSs or emails). The processing of the data subject's personal information for the purposes of direct marketing is prohibited unless the data subject has given its consent or the email recipient is a customer of the responsible party. When sending emails to a data subject who is a customer, the responsible party must have obtained the details of the data subject through a sale of a product or service, the marketing should relate to its own similar products or services and the data subject must have been given a reasonable opportunity to object to the use of its personal information for marketing when such information was collected.

The PPI Act, also prohibits automated processing of personal information where the data subject will be subjected to a decision which has legal consequences for the data subject or which affects the data subject to a substantial degree. There are certain exceptions to this prohibition.

ONLINE PRIVACY

The PPI Act as of the time of writing does not contain provisions regulating the use of cookies or location data.

KEY CONTACTS

Cliffe Dekker Hofmeyr Inc.
www.cliffedekkerhofmeyr.com/

Preeta Bhagattjee
Head of Data Protection and Privacy Group
T +2711 562 1038
preeta.bhagattjee@dlacdh.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SOUTH KOREA

Last modified 27 January 2016

LAW IN SOUTH KOREA

In the past, South Korea did not have a comprehensive law governing data privacy. However, a law relating to protection of personal information (Personal Information Protection Act, 'PIPA') was enacted and became effective as of 30 September 2011.

Moreover, there is sector specific legislation such as:

- the Act on Promotion of Information and Communication Network Utilisation and Information Protection ('IT Network Act') which regulates the collection and use of personal information by IT Service Providers, defined as telecommunications business operators under Article 2.8 of the Telecommunications Business Act; and other persons who provide information or intermediate the provision of information for profit by utilising services rendered by a telecommunications business operator

- the Use and Protection of Credit Information Act ('UPCIA') which regulates the use and disclosure of Personal Credit Information, defined as credit information which is necessary to determine the credit rating, credit transaction capacity, etc. of an individual person. The UPCIA primarily applies to Credit Information Providers/Users, defined under Article 2.7 of the UPCIA as a person (entity) prescribed by Presidential Decree thereof who provides any third party with credit information obtained or produced in relation to his/her own business for purposes of commercial transactions, such as financial transactions with customers, or who has been continuously supplied with credit information from any third party to use such information for his/her own business, and

- the Act on Real Name Financial Transactions and Guarantee of Secrecy ('ARNFTGS') which applies to information obtained by financial or financial services institutions.

Under PIPA, except as otherwise provided for in any other Act, the protection of personal information shall be governed by the provisions of PIPA.

DEFINITIONS

Definition of personal data

Under PIPA, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, images, or other similar information (including information that does not, by itself, make it possible to identify a specific person but that which enables the recipient of the information to easily identify such person if combined with other information).

Under the IT Network Act, information pertaining to a living individual, which contains information identifying a specific

person with a name, a national identification number, or similar in a form of code, letter, voice, sound, image, or any other form (including information that does not, by itself, make it possible to identify a specific person but that enables such person to be identified easily if combined with other information).

The relevant Korean authorities' understanding is that the construction of Personal Data under PIPA and that under IT Network Act are the same in spite of subtle differences in definition wordings.

Definition of sensitive personal data

Under PIPA, Sensitive Personal Data is defined as Personal Data consisting of information relating to a living individual's:

- thoughts or creed
- history regarding membership in a political party or labour union
- political views
- health care and sexual life, and
- other Personal Data stipulated under the Enforcement Decree (the Presidential Decree) which is anticipated to otherwise intrude seriously upon the privacy of the person.

The Enforcement Decree of PIPA includes genetic information and criminal record as Sensitive Personal Data. The IT Network Act also has a similar definition.

NATIONAL DATA PROTECTION AUTHORITY

The Ministry of the Interior ("MOI") is in charge of the execution of PIPA. The Korea Communications Commission ('KCC') is in charge of the execution of the IT Network Act.

REGISTRATION

Under PIPA, a public institution which manages a Personal Data file (collection of Personal Data) shall register the following with the MOI:

- name of the Personal Data file
- basis and purpose of operation of the Personal Data file
- items of Personal Data which are recorded in the Personal Data file
- the method to process Personal Data
- period to retain Personal Data
- person who receives Personal Data generally or repeatedly, and
- other matters prescribed by Presidential Decree. A 'public institution' in this context refers to any government agency or institution.

The Presidential Decree of PIPA stipulates that the followings also shall be registered with the MOI:

- the name of the institution which operates the Personal Data file

- the number of subjects of the Personal Data included in the Personal Data file
- the department of the institution in charge of Personal Data processing
- the department of the institution handling the Personal Data subjects' request for inspection of Personal Data, and
- the scope of Personal Data inspection of which can be restricted or rejected and the grounds therefore.

Only 'public institutions' are required to register with the MOI.

DATA PROTECTION OFFICERS

Under PIPA, every Data Handler (which means any person, any government entity, company, individual or other person that, directly or through a third party, handles Personal Data in order to manage Personal Data files for work purposes) must designate a data protection officer.

Under the IT Network Act, every IT Service Provider must designate a director or chief officer of the department in charge of handling Personal Data as a data protection officer. Pursuant to Presidential Decree of the IT Network Act where, an IT Service Provider has less than 5 employees, the owner or representative director shall be the person in charge.

There are no nationality or residency requirements for the data protection officer. In the event that a data protection officer is not designated, the Data Handler may be subject to a maximum administrative fine of KRW 10 million under the PIPA or KRW 20 million under the IT Network Act.

COLLECTION & PROCESSING

If a Data Handler under PIPA or an IT Service Provider under the IT Network Act intends to collect Personal Data from the data subject or IT service user, it must:

- first notify the data subject or IT service user of the vital information stipulated under the law, and
- obtain the data subject's or IT service user's prior consent to such collection other than some exceptional cases stipulated under the law.

If a Data Handler under PIPA intends to collect Sensitive Personal Information, the consent must be separately obtained.

Under the amended IT Network Act, which became effective as of 18 August 2012, an IT Service Provider shall not collect a Resident Registration number (equivalent to Social Security number in the United States), unless:

- the IT Service Provider is designated as an identification institution by the KCC, or
- there exist special provisions under any other laws or Notification of the KCC.

Under the PIPA, prior to obtaining the prerequisite consent for collecting Personal Data from a data subject, a Data Handler must notify the data subject of:

- the purpose of collection and use of Personal Data
- items of Personal Data to be collected
- time period for possession and use of Personal Data, and

- the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, prior to obtaining prerequisite consent for collecting Personal Data from an IT service user, an IT Service Provider must notify the IT service user of:

- the purpose of collection and use of Personal Data
- items of Personal Data to be collected, and
- time period for possession and use of Personal Data.

Under the newly amended PIPA, effective as of 7 August 2014, an Data Handler shall not handle a Resident Registration number, unless:

- there exists special provisions requiring or permitting the handling of the Resident Registration number under other laws
- there is clear evidence of some urgent need to handle the data, for the sake of the safety or property of the data subject or of a third party, or
- the handling of the Resident Registration number is unavoidable and there exist special provisions under ordinance of the MOI.

When a certain business transfer occurs, the Data Handler or IT service provider must provide its data subjects or IT service users a chance to opt out by providing a notice, including items of:

- the expected occurrence of Personal Data transfers
- the contact information of the recipient of the Personal Data, including the name, address, telephone number and other contact details of the recipient, and
- the means and process by which the data subject or IT service user may refuse to consent to the transfer of Personal Data.

If the data subject or IT service user is under 14, the consent of his/her legal guardian must be obtained.

As a general rule, a Data Handler under PIPA or an IT Service Provider under the IT Network Act may not handle Personal Data without obtaining the prior consent of the data subject or IT service user, beyond the scope necessary for the achievement of the Purpose of Use. This general rule also applies where a Data Handler or IT Service Provider acquires Personal Data as a result of a merger or acquisition.

Exceptions to the general rule above apply in the following cases under PIPA:

- where there exist special provisions in any Act or it is inevitable to fulfil an obligation imposed by or under any Act and subordinate statute
- where it is inevitable for a public institution to perform its affairs provided for in any Act and subordinate statute
- where it is inevitably necessary for entering into and performing a contract with a subject of Personal Data
- where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, and
- where it is necessary for a Data Handler to realise his/her legitimate interests and this obviously takes precedence over the rights of a subject of Personal Data. In such cases, this shall be limited to cases where such data is substantially relevant to a Data Handler's legitimate interests and reasonable scope is not

exceeded.

Exceptions to the general rule above apply in the following cases under the IT Network Act:

- if the Personal Data is necessary in performing the contract for provision of IT services, but it is obviously difficult to get consent in an ordinary way due to any economic or technical reason.
- if it is necessary in settling the payment for charges on the IT services rendered, and
- if a specific provision exists in this Act or any other Act.

Under the ARNFTGS, financial institutions must obtain written consent for the disclosure of an individual's information relating to his/her financial transactions.

TRANSFER

As a general rule, a Data Handler or an IT Service Provider may not provide Personal Data to a third party without obtaining the prior opt in consent of the data subject or IT service user.

Exceptions to the general rule above apply in the following cases under PIPA:

- where there exist special provisions in any Act or it is necessary to fulfil an obligation imposed by or under any Act and subordinate statute
- where it is necessary for a public institution to perform its affairs provided for in any Act and subordinate statute, etc, and
- where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.

Exceptions to the general rule above apply under the IT Network Act if a specific provision exists in this Act or any other act otherwise.

Under PIPA, a Data Handler must obtain consent after it notifies the data subject of:

- the person (entity) to whom the Personal Data is furnished
- purpose of use of the Personal Data by the person (entity)
- types of Personal Data furnished
- period of time during which the person (entity) will possess and use the Personal Data, and
- the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, an IT Service Provider must notify the IT service user of:

- the person (entity) to whom the Personal Data is furnished
- purpose of use of the Personal Data by the person (entity)
- types of Personal Data furnished, and
- period of time during which the person (entity) will possess and use the Personal Data, and then obtain consent

from the IT service user.

The UPCIA stipulates that prior to obtaining prerequisite consent for providing personal credit information to any other person, a Credit Information Provider/User must notify the credit information subject of:

- the person (entity) to whom the credit information will be furnished
- the purpose of use of the Personal Credit Information by the person (entity)
- the types of Personal Credit Information to be furnished, and
- the period of time during which the person (entity) will possess and use the Personal Credit Information.

Exceptions to the general rule above apply in the following cases under the UPCIA:

- where a Credit Information Company as defined under Article 2.5 of the UPCIA provides such information for the purpose of performing central management and utilisation thereof with another Credit Information Company or Credit Information Collection Agency as defined under Article 2.6 of the UPCIA
- where such provision is required to perform a contract, and to entrust the processing of credit information under Article 17.2 of the UPCIA
- where the relevant Personal Credit Information is provided as part of rights and obligations that are transferred by way of business transfer, division, merger, etc
- where Personal Credit Information is provided for a person who uses the information for purposes prescribed by Presidential Decree, including claims collection (applicable only to the credit which is an object of collection), license and authorisation, determination of a company's credit worthiness, and transfer of securities
- where Personal Credit Information is provided in accordance with a court order for submission thereof or a warrant issued by a judicial officer
- where such information is provided upon the request of a prosecutor or judicial police officer, in the event of occurrence of an emergency where a victim's life is in danger or he/she is expected to suffer bodily injury, etc., so that no time is available to issue a judicial warrant
- where such information is provided as the head of a competent government office requests, in writing, for the purpose of inquiry and examination in accordance with any laws pertaining to taxes or demands the taxation data required to be provided in accordance with such laws pertaining to taxes
- where Personal Credit Information held by a financial institution is provided to a foreign financial supervisory body in accordance with international conventions, etc, and
- where such information is otherwise provided in accordance with other laws.

Under the ARNFTGS, financial institutions must obtain written consent for the transfer of an individual's information relating to his/her financial transactions to a third party.

SECURITY

Under PIPA and IT Network Act, every Data Handler or IT Service Provider must, when it handles Personal Data of a data subject or IT service user, take the following technical and administrative measures in accordance with the guidelines prescribed by Presidential Decree to prevent loss, theft, leakage, alteration, or destruction of Personal Data:

- establishment and implementation of an internal control plan for handling Personal Data in a safe way
- installation and operation of an access control device, such as a system for blocking intrusion to cut off illegal access to Personal Data
- measures for preventing fabrication and alteration of access records
- measures for security including encryption technology and other methods for safe storage and transmission of Personal Data
- measures for preventing intrusion of computer viruses, including installation and operation of vaccine software, and
- other protective measures necessary for securing the safety of Personal Data.

BREACH NOTIFICATION

Under PIPA, if a breach of Personal Data occurs the Data Handler must notify the data subjects without delay of the details and circumstances, and the remedial steps planned. If the number of affected data subjects exceeds 10,000, the Data Handler shall immediately report the notification to data subjects and the result of measures taken to MOI, KISA or the National Information Security Agency ('NIA').

Under the IT Network Act, an IT Service Provider must, if it discovers an occurrence of intrusion:

- report it to the KCC or the Korea Internet & Security Agency (KISA) within twenty four (24) hours of knowledge of the intrusion, and
- analyse causes of intrusion and prevent damage from being spread, whenever an intrusion occurs.

The KCC may, if deemed necessary for analysing causes of an intrusion, order an IT Service Provider to preserve relevant data, such as access records of the relevant information and communications network.

Under the newly amended IT Network Act, which became effective as of 29 November 2014, if a loss, theft or leakage of Personal Data occurs, the IT Service Provider must notify the IT Service user immediately and report to the KCC within twenty four (24) hours of the details and circumstances, and the remedial steps planned.

ENFORCEMENT

The competent authorities may request reports on the handling of Personal Data, and also may issue recommendations or orders if a Data Handler or IT Service Provider violates PIPA or the IT Network Act. Non compliance with a request or violation of an order can result in fines, imprisonment, or both.

For example, MOI, the supervising authority for Data Handlers, can issue a corrective order in response to any breach of an obligation not to provide Personal Data to a third party. Breach of a corrective order leads to an administrative fine of not more than KRW 30 million. Prior to issuing a corrective order, MOI may take an incremental approach and instruct, advise and make recommendations to the Data Handler.

Under the IT Network Act, an IT Service Provider who collected Personal Data without consent of the relevant user shall be subject to the penalty of imprisonment for not more than 5 years or a fine not exceeding KRW 50 million.

Under the UPCIA, a Credit Information Provider/User who has provided Personal Credit Information without consent of the relevant credit information subject shall be subject to the penalty of imprisonment of up to 5 years or a fine not exceeding KRW 50 million.

Under the ARNFTGS, a person who discloses information or data concerning financial transactions shall be punished

by imprisonment not exceeding 5 years or by a fine not exceeding KRW 30 million.

PUNITIVE DAMAGES

In the event that a Credit Information Provider/User suffers any damages resulting from the Data Handler's conduct, the Credit Information Provider/User may bring a claim against the Data Handler for such damages. In such cases, a Data Handler may not be discharged from liability unless it can prove that there was no intentional act nor negligence on its part.

As of July 25, 2016, as a result of an amendment to PIPA, in instances Personal Data breaches caused by the Data Handler's intentional act or negligence, the Data Handler may be liable for three times the damages suffered.

ELECTRONIC MARKETING

The transmission of an advertisement via an information and communication network, including electronic mails is not prohibited by the IT Network Act, but provides individuals with the right to prevent the processing of their personal data (eg a right to 'opt out') for electronic marketing purposes. An IT Service Provider who intends to transmit an advertisement by information and communication network must receive the explicit consent of the individual, but if the individual either withdraws consent or does not give consent, then an advertisement with commercial purposes may not be transmitted.

In addition, the transmitter of advertisement information for commercial purposes must disclose the following specifically within the advertisement information:

- the identity and contact information of the transmitter
- instructions on how to consent or withdraw consent for receipt of the advertisement information

A person who transmits an advertisement shall not take any of the following technical measures:

- a measure to avoid or impede the addressee's denial of reception of the advertising information or the revocation of his consent to receive such information
- a measure to generate an addressee's contact information, such as telephone number and electronic mail address, automatically by combining figures, codes, or letters
- a measure to register electronic mail addresses automatically with intent to transmit advertising information for profit, and
- various measures to hide the identity of the sender of advertising information or the source of transmission of an advertisement.

ONLINE PRIVACY

Cookie, log, IP information, etc. are also regulated by the IT Network Act as personal data, which if combined with other information enable the identification of a specific individual person easily. Under the IT Network Act, using cookies (or web beacons) must be done with the opt-out consent of the user and the privacy policy must publicise the matters concerning installation, operation and opt-out process for automated means of collecting personal information, such as cookies, logs and web beacons.

The protection of location information is governed by the provisions of the Act on the Protection, Use, etc. of Location Information ('LBS Act').

Under the LBS Act, any person who intends to collect, use, or provide location information of a person or mobile object shall obtain the prior consent of the person or the owner of the object, unless:

- there is a request for emergency relief or the issuance of a warning by an emergency rescue and relief agency
- there is a request by the police for the rescue of the person whose life or physical safety is in immediate danger, or
- there exist special provisions in any Act.

Under the LBS Act, any person (entity) who intends to provide services based on location information (the 'Location-based Service Provider') shall report to the KCC. Further, any person (entity) who intends to collect location information and provide the collected location information to location-based service providers (the 'Location Information Provider') shall obtain a license from the KCC.

If a Location Information Provider intends to collect personal location information, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information:

- name, address, phone number and other contact information of the Location Information Provider
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights
- details of the services the Location Information Provider intends to provide to Location-based Service Providers
- grounds for and period of retaining data confirming the collection of location information, and
- methods of collecting location information.

If a Location-based Service Provider intends to provide location-based services by utilising personal location information provided from a Location Information Provider, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information:

- name, address, phone number and other contact information of the Location-based Service Provider
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights
- details of the Location-based Services
- grounds for and period of retaining data confirming the use and provision of location information, and
- matters concerning notifying the personal location information subject of the provision of location information to a third party as below.

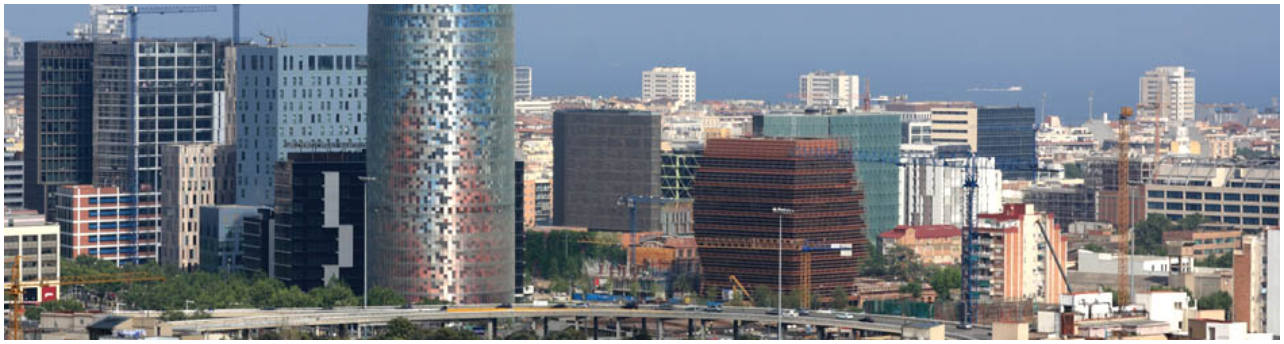
If a Location-based Service Provider intends to provide location information to a third party, in addition to the above, it must notify the subjects of personal location information of the third party who will receive the location information and the purpose of this provision.

KEY CONTACTS

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SPAIN



Last modified 19 October 2015

LAW IN SPAIN

As a member of the European Union, Spain formally implemented the EU Data Protection Directive 95/46/EC in November 1999 with the Special Data Protection Act 1999 (the 'Act', also known as the 'LOPD' in Spain). Nevertheless, from 1992, Spain already had a Data Protection Act ('LORTAD') that was fully consistent with most of the contents of the EU Data Protection Directive 95/46/EC. The Act, simply represents an up-to-date version of LORTAD, rather than being a major change in the legal framework. Enforcement is through the Spanish Data Protection Commissioner's Office ('AEPD'). Its last amendment took place in March 2011.

DEFINITIONS

Definition of personal data

Any information (including numbers, text, graphics, pictures, video, sounds or any other type of data) related to individuals that are identified or identifiable.

Definition of sensitive personal data

Personal data related to political orientation, religion, beliefs, trade union membership, ethnic origin, health and sex life. Each category of sensitive information enjoys, however, a different level of protection. Of note, criminal/administrative infringements data can be included only in the databases of certain public authorities, with individuals and companies being forbidden to do so, whilst other categories allow collection and processing under certain conditions.

NATIONAL DATA PROTECTION AUTHORITY

The Spanish Data Protection Commissioner's Office ('AEPD', standing in Spanish for *Agencia Española de Protección de Datos*). It is based in Madrid. Regional commissioners may exist as well in certain territories, dealing only with data protection issues of the regional public authorities themselves.

REGISTRATION

Unlike other EU Member States, Spain does not maintain a register of controllers or of processing activities. Instead, the AEPD holds a registry of databases containing personal information. Registration, carried out through state of the art software provided by the AEPD (called 'NOTA'), is very detailed and identifies in full not only the data controller, but also any data processors supporting it. It contains a clear description of the database contents, the sources of the data, the purposes for which the data is collected, processed and transferred, as well as the identity of the recipients of the information, with special attention paid to international transfers. Any changes to the database require the registration to be amended.

DATA PROTECTION OFFICERS

Although there is no blanket requirement in Spain for organisations to appoint a data protection officer as such, organisations handling personal information to which 'medium' or 'high' security requirements apply shall appoint a Head of Data Security. The Head of Data Security is not in charge of data protection matters in general, but only the security measures to be applied to databases.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject consents
- the data controller needs to process the data to enter into or carry out a contract or pre contractual deal to which the data subject is a party so that the contract or deal can be maintained or executed
- the data is collected from 'public open sources' (although the requirement of arising from 'public open sources' has been challenged by the courts) and the processing is necessary to satisfy a legitimate interest of the data controller or a third party receiving the data, provided that the constitutional basic rights of the data subject are preserved
- the processing protects the data controller's vital interests, or
- the processing is required by an enactment or to legitimately perform a public function in the public interest.

Where sensitive personal data is processed, one of the above conditions must be met plus one further condition from a separate list of more stringent conditions (explicit and written consent in the case of political, moral and religious beliefs and trade union membership or explicit consent from the data subject plus general interest grounds supported by a law, in the case of ethnic origin, health and sex life).

The data controller shall provide the data subject with 'fair processing information'. This includes the existence of a database storing his/ her personal data, the identity and address of the data controller, the purposes of processing, the consequences of supplying/refusing to supply the information, whether it is mandatory or not to supply the information requested, and how the data subject may exercise the rights of access, modification, cancellation and objection to the data.

TRANSFER

Data controllers may transfer personal data to third parties (group companies being considered third parties for this purpose) if any of the following conditions are met:

- the data subject consents
- the transfer is endorsed by a law
- the data is collected from 'public open sources'
- the transfer to a third party is essential to a contract to which the data subject has become freely and legitimately a party
- the transfer is intended for the national or regional Ombudsman (*Defensor del Pueblo*), Public Prosecutor, Judges and Courts, and the Public Finances Court, within their legal faculties
- the transfer takes place between public bodies and is intended for historical, statistical or scientific research, or

- the transfer is urgently needed to protect the health of the data subject or other individuals.

Consent can be revoked at any time and will be void if the information provided to the data subject did not allow them to determine the purposes for which the data should be used, or the scope of the activities of the recipient.

These principles apply to transfers within Spain or within the European Economic Area. Transfers of a data subject's personal data to non EU/European Economic Area countries is similarly allowed under the following circumstances:

- those countries providing 'adequate protection' for the security of the data (eg Argentina)
- if the transfer takes place under a Treaty to which Spain is a party
- if it is intended to provide or to request international judiciary cooperation
- if the transfer is required for serious medical matters
- if it refers to international money transfers
- if the data subject consents to it in a unequivocal manner
- if the transfer is necessary to execute a contract or a pre-contractual deal between the data subject and the data controller upon a request of the former
- if the transfer is necessary to execute, in the interests of the data subject, a contract between the data controller and a third party
- if the transfer is necessary to protect a public interest
- if the transfer is necessary for the enforcement, exercise or defence of a right at court, or
- if the transfer takes place from a Public Registry for a legitimate purpose and to a legitimate recipient, following the instructions of a legitimated person.

In any other case, the transfer abroad to non-adequate territories must be authorised in advance by the AEPD (the use of 'standard contractual clauses' approved by the European Commission, or the implementation of Binding Corporate Rules easing the granting of such approval).

For the transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of the AEPD. Consent clauses, however, are deemed valid only if they explicitly mention that the recipient is based in the US and that data protection laws there do not offer a level of privacy protection equivalent to that applied within the EU.*

Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.

SECURITY

Data controllers and processors must take appropriate technical and organisational measures against unauthorised or unlawful access or processing, and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the nature of the data. 'Basic' security measures must be

applied to all data, and include, *inter alia*, control of access to data by employees of the data controller. 'Medium' security measures must be applied to data relating to financial services, public security, public tax matters or which may allow data controllers to profile a data subject in detail. These measures include, inter alia, the execution of privacy audits every two years and the appointment of a Head of Data Security. Databases containing sensitive information (as well as data relating to gender violence, and police records) require 'high' security measures, including, inter alia, tougher access control and data encryption when communicating the data.

BREACH NOTIFICATION

As of yet, there is no mandatory requirement in the LOPD to report data security breaches or losses to the AEPD or to data subjects. Nevertheless, the organisation is required to record such incidents in the Security Incidents Ledger. The AEPD is entitled to request to see the Security Incidents Ledger at any time. As a matter of fact, Police Forces and Public Offices do normally immediately report to the AEPD any data breach or loss of personal data they may be informed about (eg when a claim for the theft of a hard disk is filed by the owner). In March 2012, the Spanish General Telecommunications Act was amended to oblige telecommunications operators to rapidly report data breaches to AEPD and to the relevant data subjects. Rumours on the possibility of extending that obligation to other companies have been heard, but this has not happened to date.

ENFORCEMENT

In Spain, the AEPD is responsible for enforcement of the Act. Acting either *ex officio* or upon a complaint from a data subject (or a public authority, for example the Consumer Protection Office to which the data subject has complained), the AEPD is entitled to start:

- an investigation procedure, to collect information
- a privacy rights protection procedure, when a data controller is refusing to allow a data subject to exercise his/her access, rectification, cancellation or objection rights, and
- a disciplinary procedure when enough evidence has been gathered to suspect that a data controller has infringed the LOPD.

Although the AEPD did not issue in the past any 'warnings' to the data controllers asking them to comply with the law, following recent legal amendments AEPD has resorted often to this mechanism (only for less serious cases and when no prior warnings had been issued before to the same data controller for any data protection matter, however). The first notice that an organisation may receive in many cases from the AEPD is the commencement of a disciplinary procedure.

Sanctions are essentially monetary fines. They range from EUR 900 to EUR 40,000 for minor infringements, EUR 40,001 to EUR 300,000 for serious infringements and EUR 300,001 to EUR 600,000 for very serious infringements. Very serious and serious infringements are more frequently detected and sanctioned than minor ones. The fines stated here are per infringement, but very often fines are aggregated within a given case to form a larger total fine.

ELECTRONIC MARKETING

Electronic Marketing is regulated in Spain, in addition to the Spanish Data Protection Act, by the Spanish Act on the Information Society Services and e-Commerce ('LSSI'), as amended in March 2012. The general principle is that deliveries of electronic marketing materials are lawful only if they have been explicitly authorised in advance by the recipients (authorisation that is required not just for individuals, but also when the recipient is a legal entity, broadening here the scope of Spanish Data Protection Act). An exception to this general principle applies to deliveries to clients when the materials refer to products/services that are equal or similar to the ones sold to them in the past by the company sponsoring the advertisement.

Electronic publicity shall:

- be clearly marked as such by means of the terms PUBLI or PUBLICIDAD placed inside the subject line
- allow the recipient to opt-out at all times, even by the time of registration, and
- clearly identify the sponsor of the delivery. It is the sponsor of the delivery, not the electronic publicity company that shall be held liable in case of enforcement. Opt-out shall include an email address when the publicity was delivered by email too. Opt-out procedure shall be simple and free for the recipient of the publicity.

Enforcement shall include, inter alia, fines that, in most cases, shall be between EUR 30,000 and EUR 150,000.

ONLINE PRIVACY

Cookies are regulated in Spain, in addition to the Spanish Data Protection Act, by the Spanish Act on the Information Society Services and e-Commerce ('LSSI'), as amended in March 2012. By the end of April 2013, the AEPD has released Guidance Notes on the use of cookies. Although the Guidance Notes are not legally binding they give useful indications on the best market practice and on the criteria that the AEPD would follow when enforcing the law.

The new regulation requires data controllers to inform cookies' recipients (referred to in the LSSI as giving users the 'actual opportunity') – including legal entities – of the existence and use of cookies, their scope and how to deactivate them. Actual opportunity is interpreted by the regulator as a procedure by which the user cannot browse the website, for example, without noticing the invitation to review the above-mentioned information and carrying out an active behaviour (even a simple one like pressing the ESC key) to continue browsing after being presented with the information or the opportunity to review it. A semi-transparent layer on the usual homepage screen is a generally approved mechanism to request the consent (although AEPD has indicated in some reports released in 2014 that a two-step warning approach may work best (first warning on the landing page containing the basics, second one on a separate cookies policy including full details). Certain types of cookies (eg session cookies) are exempt from these restrictions as per the WP29 criteria released during the summer of 2012. The Spanish AEPD has made known to the public, by the way of a resolution, that in some cases the delivery of cookies to the computer of a user based in Spain may trigger the application of Spanish Data Protection Act in full.

On location data, the local position is that it may be acceptable provided that:

- users are informed at all times on whether the location system is active
- users have agreed to be located, and
- users have the option (especially when being off-duty if the location data is used in an employment context) to turn off the system.

KEY CONTACTS

Diego Ramos
Partner
T +349 17901658
diego.ramos@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SWEDEN

Last modified 12 January 2016

LAW IN SWEDEN

Being a member of the European Union, Sweden implemented the EU Data Protection Directive 95/46/EC in 1998 with the Personal Data Act (Sw. *personuppgiftslagen*, SFS 1998:204, below 'the Act'). The previous Swedish Data Act enacted in 1973 had by then already been considered to be outdated for many years.

DEFINITIONS

Definition of personal data

Personal data means all kinds of information that is directly or indirectly referable to a natural living person.

Definition of sensitive personal data

Sensitive personal data means personal data that discloses race or ethnic origin, political opinions, religious or philosophical convictions and membership of trade unions. Personal data relating to health or sexual life is also embraced by the term.

NATIONAL DATA PROTECTION AUTHORITY

The Data Inspection Board (Sw. *Datainspektionen*, below 'DIB') is the supervisory authority under the Act.

Contact details:
Datainspektionen
Drottninggatan 29, plan 5
Box 8114
104 20 Stockholm

T +46 8 657 61 00

datainspektionen@datainspektionen.se

REGISTRATION

All controllers except those whose processing falls under any of the exemptions in the Act, need to file notifications with the DIB.

Notification is *not* required if:

- the controller has appointed a personal data representative (a data protection officer or 'Privacy Officer') and

notified the DPA about this, or

- the processing would probably not result in an improper intrusion of personal integrity, if specified in rules issued by either the Government or the DIB (for instance processing of personal data in running text, processing takes place with the individuals consent, or the data relates to a registered person who has a link to the controller such as members, employees, customers).

DATA PROTECTION OFFICERS

There is no requirement in Sweden for organisations to appoint a data protection officer. It is a voluntary arrangement. However, if a data protection officer has been appointed and notified to the DIB, the general notification obligation does not apply. Instead, the officer has to maintain a register of the processing that the data controller implements and which would have been subject to the notification duty if the data protection officer had not existed.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject consents
- there is statutory authority for the processing
- the processing is necessary to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract
- the processing is necessary to enable the controller to fulfil a legal obligation
- the processing is necessary to protect the vital interests of the data subject
- the processing is necessary to perform a task in the public interest
- the processing is necessary to exercise official authority, or
- to satisfy a purpose that concerns a justified interest on the part of the controller or on the part of a third party to whom the personal data is disclosed, provided that this interest outweighs the registered person's interest in protection against violation of personal integrity.

In relation to processing of sensitive personal data, additional requirements apply apart from what has been mentioned above.

Whichever of the above conditions is relied upon, the controller must first provide the data subject with certain information, unless an exemption applies. The notification shall include information on the identity of the controller, the purposes of the processing, whether the data will be disclosed and/or transferred and to who/where, the fact that the provision of data is voluntary and any other circumstances that will enable the data subject to exercise his/her rights pursuant to the Act.

TRANSFER

In principle, it is forbidden to transfer personal data that is being processed to a country outside the EU/EEA that does not have an adequate level of protection for personal data.

Even if the third country in question does not have an adequate level of protection, it is allowed to transfer personal data to such country if the registered person has given his/her consent to the transfer or when the transfer is necessary in order that:

- a contract between the registered person and the controller may be performed or measures that the registered person requested may be taken before a contract is made
- a contract between the controller and a third party that is in the interests of the registered person may be made or performed
- legal claims should be established, exercised or defended, or
- vital interests of the registered person may be protected.

It is also permitted to transfer personal data for use solely in a state that has acceded to the Council of Europe Convention of 28 January 1981 on the protection of individuals in automatic data processing.

Transfer of personal data to third countries is allowed if the countries provide 'adequate protection' for the security of the data, or if the transfer is covered by standard contractual clauses approved by the European Commission, or subject to an organisation's Binding Corporate Rules.

As a result of the Court of Justice of the European Union's (ECJ) judgment on 6 October 2015 in the case of Schrems (C-362/14) the US-EU Safe Harbor regime is no longer regarded as a valid basis for transferring personal data from Sweden to the US. The DIB has yet to issue any detailed guidance on the matter. To our knowledge the DIB has not taken any enforcement actions against any data controllers following the ECJ's judgment.

Please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.

SECURITY

The data controller is liable to implement technical and organisational measures to protect the personal data. The measures shall attain a suitable level of security. When the controller engages a data assistant to conduct the processing of personal data (data processor), there shall be a written contract that specifically regulates the security aspects. The controller shall also be responsible to ensure that the assistant actually implements the necessary security measures.

It is the controller who is responsible in relation to the registered person as regards the processing, even if an assistant/processor has been engaged or if someone who works for the controller has wrongfully disclosed personal data.

The DIB may issue decisions on security measures in individual cases.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the DIB. Data security breaches are handled on a case-by-case basis and addressed by the DIB only if they for instance relate to a large number of data subjects or indicate a general non-compliance issue. There is no DIB guidance on the subject matter.

However, pursuant to the implementation of the ePrivacy Directive as amended, regarding security breach notification obligations, chapter 6 of the Swedish Electronic Communications Act (Sw. *lag om elektronisk kommunikation*, SFS 2003:389) as of July 2011 provides that a provider of publicly available electronic communications services shall without undue delay notify the Swedish Post and Telecom Authority (Sw. *Post och Telestyrelsen*) regarding privacy incidents. Where the incident is likely to adversely affect subscribers or users of whom the processed data concerns, or where the Post and Telecom Authority requests it, the provider shall also notify subscribers without undue delay. Incidents that only have a marginal effect on subscribers and users do not have to be notified to the authority. Moreover, notification is not required where the service provider has implemented appropriate security measures which renders the data unreadable to unauthorised persons.

ENFORCEMENT

The DIB has, in its capacity as the supervisory authority, the right of access to the personal data processed and information about and the documentation of processing, and is also empowered to enter premises connected with the processing.

Appeal may be made against a decision by the DIB to a general administrative court; ie in the first instance the County Administrative Court. The DIB may decide that a decision should apply even if it is appealed against.

A person who has intentionally or by gross negligence disclosed untrue data under the Act, who in contravention of the regulations processes sensitive personal data or data concerning offences, etc., or transfers personal data to a third country or neglects to give notice concerning the processing to the supervisory authority may be sentenced to a fine or imprisonment of at most six months. If the offence is grave, the penalty may be imprisonment up to two years. A sentence shall not be imposed in petty cases.

Furthermore, the controller may also be liable to pay compensation to a registered person for damage and violation of personal integrity caused by the processing of personal data in contravention of the Act.

ELECTRONIC MARKETING

The Act applies to most electronic marketing activities, given that it is likely that such marketing involves processing of personal data (eg an e-mail address is likely regarded as personal data under the Act). Please note that if the data subject's e-mail address has not been obtained in the context of a customer relationship or similar, the data subject's consent is, as a main rule, required for electronic marketing. Moreover, a data subject has a right to at any time oppose ('opt-out' of) further processing of his or her personal data for marketing purposes.

ONLINE PRIVACY

Pursuant to the Swedish Electronic Communications Act (as amended by e-Privacy Directive 2009/12/EC), a cookie may be stored on a user's terminal equipment, only if the user has been given access to information on the purpose of the processing and given his or her consent, ie the user must give his/her prior 'opt-in' consent before a cookie is placed on the user's computer. The government stated in the preparatory works to the Swedish Electronic Communications Act that the implementation of the new e-Privacy Directive should not be regarded as a material change. This has been construed by some that implied consent through browser settings shall be regarded as a valid consent under the Act, provided that sufficient information is given to the user eg in a cookie policy. This is, however, unclear and the Swedish Post and Telecom Authority has not issued any guidance in this regard.

Consent is, however, not required for cookies that are:

- used for the sole purpose of carrying out the transmission of communication over an electronic communications network, or
- necessary for the provision of a service explicitly requested by the user.

Wilful or negligent breach of the Swedish Electronic Communications Act in this regard is sanctioned with fines, provided that the offence is not sanctioned by the Swedish Criminal Code (Sw. *brottsbalken*). However, if the breach is deemed to be minor, no sanction shall be imposed. To our knowledge there has been no case where a website operator has been fined for breach of the Swedish Electronic Communications Act.

KEY CONTACTS

DLA Nordic
www.dlanordic.se/

Johan Sundberg
Advokat/Partner
T +46 8 769 79 30
johan.sundberg@dlanordic.se

Johan Thörn
Jur. kand/Associate
T T +46 8 769 79 30
johan.thorn@dlanordic.se

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

SWITZERLAND

Last modified 12 January 2016

LAW IN SWITZERLAND

The processing of personal data is mainly regulated by the Federal Act on Data Protection of 19 June 1992 ('DPA') and its ordinances, ie the Ordinance to the Federal Act on Data Protection ('DPO') and the Ordinance on Data Protection Certification ('ODPC').

In addition, the processing of personal data is further restricted by provisions in other laws, mainly with regard to the public sector and regulated markets.

DEFINITIONS

Definition of personal data

Personal data means all information relating to an identified or identifiable natural or legal person.

Definition of sensitive personal data

Sensitive personal data is defined as data on:

- religious, ideological, political or trade union related views or activities
- health, the intimate sphere or racial origin
- social security measures, and
- administrative or criminal proceedings and sanctions.

'Personality profiles' are protected to the same extent under the DPA as sensitive personal data. Personality profiles are collections of data that allow the appraisal of essential characteristics of the personality of an individual.

NATIONAL DATA PROTECTION AUTHORITY

Federal Data Protection and Information Commissioner ('FDPIC')

Feldeggweg 1
CH 3003 Berne
Switzerland

T +41 (0)58 462 43 95
F +41 (0)58 465 99 96

The FDPIC supervises federal and private bodies, advises and comments on the legal provisions on data protection and assists federal and cantonal authorities in the field of data protection.

The FDPIC informs the public about his findings and recommendations, and maintains and publishes the register for data files.

REGISTRATION

The processing of personal data by private persons does not usually have to be notified or registered, respectively. However, private persons must register their data files before the data files are opened, if:

- they regularly process sensitive personal data or personality profiles, or
- they regularly disclose personal data to third parties,

and unless one of the following exemptions applies:

- the data is processed pursuant to a statutory obligation
- the Swiss Federal Council has exempted the particular processing from the registration requirement because it does not prejudice the rights of the data subjects
- the data controller uses the data exclusively for publication in the edited section of a periodically published medium and does not pass on any data to third parties without informing the data subjects
- the data is processed by journalists who use the data file exclusively as a personal work aid
- the data controller has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files, or
- the data controller has acquired a data protection quality mark under a certification procedure according to Article 11 DPA and has notified the FDPIC of the result of the evaluation.

DATA PROTECTION OFFICERS

There is no requirement under Swiss data protection law to appoint a data protection officer.

However, a data controller can be dispensed from registering its data files if it has designated a data protection officer who:

- carries out his/her duties autonomously and independently
- has a certain level of expertise that is appropriate for the relevant data processing at the company (whereas it is not relevant whether or not the respective expertise was acquired in Switzerland)
- must check and audit the processing of personal data within the company
- must be in a position to recommend corrective measures when detecting any breaches of applicable data protection rules
- must have access to all data files and all data processing within the company as well as to all other information that he/she requires to fulfil his/her duties
- must maintain records of all data files controlled by the company and provide this list to the FDPIC or affected

data subjects upon request, and

- may not carry out any other activities that are incompatible with his/her duties as data protection officer.

The data controller must notify the FDPIC of the appointment of a data protection officer and thereupon will be listed on the public list of companies exempt from the requirement to register their data files.

COLLECTION & PROCESSING

The following principles apply to the collection and processing of personal data (including data of legal entities):

- personal data may only be processed lawfully, in good faith and according to the principle of proportionality
- the collection of personal data and, in particular, the purpose of its processing must be evident to the data subject
- personal data should only be processed for a purpose that is indicated or agreed at the time of collection, evident from the circumstances at the time of collection, or provided for by law
- the data controller and any processor must ensure that the data processed is accurate
- personal data must not be transferred abroad if the privacy of the data subject may be seriously endangered (see below)
- personal data must be protected from unauthorised processing by appropriate technical and organisational measures
- personal data must not be processed against the explicit will of the data subject, unless this is justified by:
    - the consent of the data subject (which must be given voluntarily and based on adequate information)
    - an overriding private or public interest, or
    - law, and
- sensitive personal data or personality files must not be disclosed to a third party, unless this is justified by:
    - the consent of the data subject (which must be given expressly in addition to being voluntary and based on adequate information)
    - an overriding private or public interest, or
    - law.

TRANSFER

Personal data may be disclosed outside Switzerland if the destination country offers an adequate level of data protection. The FDPIC maintains and publishes a list of such countries.

The FDPIC deems the data protection legislation of all EU and EEA countries to be adequate with regard to personal data of individuals. With regard to personal data of legal entities, only a few EU countries, such as Austria and Liechtenstein, are deemed to provide an adequate level of data protection.

In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:

- sufficient safeguards, such as data transfer agreements, or other contractual clauses, ensure an adequate level of protection abroad. Data transfer agreements or other contractual clauses must be notified and submitted to the FDPIC whereas mere information is sufficient if model clauses approved by the FDPIC are used.
- for transfers to the USA based on data transfer agreements or other contractual clauses, the following additional two requirements must be complied with (transition period until end of January 2016):
    - data subjects must be informed that their data is being transferred to the USA and that there is a possibility that the authorities there may access them; and
    - the contractual parties shall undertake to support affected data subjects to exercise their rights vis-à-vis foreign authorities in any way possible.
- *Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14), the FDPIC declared that it deems the US-Swiss Safe Harbor Framework (which mirrors the US-EU Safe Harbor Framework) inadequate with a view to guaranteeing adequate protection of personal data and advised relying on other measures such as contractual safeguards and binding corporate rules, with the additional requirements described above. Meanwhile, the Swiss Federal Council has issued a statement saying that it does not intend to suspend or cancel the US-Swiss Safe Harbor Agreement for the time being and is distancing itself from the position of the FDPIC. The developments in Europe with regard to the Safe Harbor Framework as well as to the EU model clauses are closely followed by the FDPIC and the Swiss Federal Council and will have an impact on their positions with regard to the requirements for transfers of data to the USA*
- there are binding corporate rules that ensure an adequate level of data protection in cross border data flows within a single legal entity or a group of companies. Such rules must be notified to the FDPIC
- the data subject consents to the particular data export (consent must be given for each individual case, a generic consent is not sufficient)
- the processing is directly connected with the conclusion or performance of a contract with the data subject
- disclosure is essential in order to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal rights before the courts
- disclosure is required in order to protect the life or the physical integrity of the data subject, or the data subject has made the personal data publicly accessible and has not expressly prohibited its processing.

SECURITY

The data controller and any processor must take adequate technical and organisational measures to protect personal data against unauthorised processing and ensure its confidentiality, availability and integrity. In particular, personal data must be protected against the following risks:

- unauthorised or accidental destruction
- accidental loss
- technical errors
- forgery, theft or unlawful use, and
- unauthorised altering, copying, accessing or other unauthorised processing.

The technical and organisational measures must be appropriate, in particular with regard to the purposes of the data processing, the scope and manner of the data processing, the risks for the data subjects and the current technological standards.

BREACH NOTIFICATION

There is no explicit statutory requirement to notify the FDPIC or the affected data subjects of data security breaches under the DPA. However, depending on the scale and severity of a breach, a notification of the data subjects may be necessary based on the data controller and processor's obligation to ensure data security (to avoid further damage), the principle of good faith or pursuant to contractual obligations.

ENFORCEMENT

The FDPIC does not have specific direct powers to enforce the DPA. He may investigate cases on his own initiative or at the request of a third party and may issue recommendations that a specific data processing practice be changed or abandoned. If the FDPIC's recommendation is not complied with, he may refer the matter to the Swiss Federal Administrative Court for a decision.

Furthermore, the DPA provides for criminal liability and fines of up to CHF 10,000 if a private person intentionally fails to comply with the following obligations under the DPA:

- duty to provide information when collecting sensitive data and personality profiles
- duty to safeguard the data subject's right to information
- obligation to notify the FDPIC with regard to contractual clauses or binding corporate rules in connection with the data transfers abroad
- obligation to register data files, or
- duty to cooperate in an FDPIC investigation.

Criminal proceedings must be initiated by the competent cantonal prosecution authority.

Finally, under Swiss civil law the data subject may apply for injunctive relief and may file a claim for damages as well as satisfaction and/or surrender of profits based on the infringement of its privacy.

ELECTRONIC MARKETING

Electronic marketing practices must comply with the provisions of the Swiss Federal Act against Unfair Competition ('UCA').

With regard to the sending of unsolicited automated mass advertisement (which, in addition to emails, includes SMS, automated calls and fax message(s)), the UCA generally requires prior consent by the recipient, ie 'opt-in'. As an exception, mass advertisings may be sent without the consent of the recipient:

- if the sender received the contact information in the course of a sale of his products or services
- if the recipient was given the opportunity to refuse the use of his/her contact information upon collection (opt-out), and
- if the mass advertising relates to similar products or services of the sender.

In addition, mass advertising emails must contain the sender's correct name, address and email contact and must provide for an easy-access and free of charge 'opt-out' from receiving future advertisements.

The UCA generally applies to business-consumer relationships as well as to business-business relationships, ie, mass advertisements sent to individuals and to corporations are subject to the same rules.

Direct marketing by telephone is lawful in Switzerland as long as it is not done in an aggressive way (eg by repeatedly calling the same person). However, art. 3 para. 1 lit. u UCA prohibits direct marketing by telephone to people who do not wish to receive commercial communication and have expressed that wish (ie opted-out) by having their entry marked in the telephone books and online telephone registers (eg through an asterisk next to their name).

In addition to the rules of the UCA, the general data protection principles under the DPA also apply with regard to electronic marketing activities, eg the collection and maintenance of email addresses or processing of any other personal data.

ONLINE PRIVACY

In general, the processing of personal data in the context of online services is subject to the general rules pertaining to the collection of personal data under the DPA. In addition, certain aspects of online privacy are covered by other regulations, such as the use of cookies which is also subject to the Swiss Telecommunications Act ('TCA').

Under the TCA, the use of cookies is considered to be processing of data on external equipment, eg another person's computer. Such processing is only permitted if users are informed about the processing and its purpose as well as about the means to refuse the processing, eg by configuring their web browser to reject cookies.

In addition, the general rules under the DPA apply where cookies collect data related to persons who are identified or identifiable, ie, personal data. The collection of personal data through cookies as well as the purpose of such a collection must be evident to the data subject. The personal data collected may only be processed for the purpose:

- indicated at the time of collection
- that is evident from the circumstances, and
- that is provided for by law.

Where the personal data collected through a cookie is:

- considered sensitive data, eg data regarding religious, ideological, political views or activities, or
- so comprehensive that it forms a personality profile, ie permits an assessment of essential characteristics of the personality of a person

the stricter rules pertaining to the processing of sensitive personal data are applicable.

These stricter rules provide, inter alia, that the data subject must be informed of:

- the identity of the data controller
- the purpose of data processing, and
- the categories of data recipients if the data shall be disclosed to third parties.

Further, in relation to the processing of sensitive personal data implied consent is not sufficient; consent must be given expressly.

KEY CONTACTS

Schellenberg Wittmer Ltd
www.swlegal.ch/

Christine Beusch-Liggenstorfer
Of Counsel/Attorney at Law
T +41 (0)44 215 5272
christine.beusch@swlegal.ch

Nadin Schwibs
Senior Associate/Attorney at Law
T +41 (0)44 215 9335
nadin.schwibs@swlegal.ch

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

TAIWAN

Last modified 28 January 2015

LAW IN TAIWAN

The former Computer Processed Personal Data Protection Law ('CPPL') was renamed as the Personal Data Protection Law ('PDPL') and amended on 26 May 2010. The PDPL became effective on 1 October 2012, except that the provisions relating to sensitive personal data and the notification obligation for personal data indirectly collected before the effectiveness of the PDPL remain ineffective. The government has proposed further amendment to these provisions, which is pending legislative review. The information hereunder is based upon the effective PDPL only.

DEFINITIONS

Definition of personal data

According to PDPL, personal data means the name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health checks, criminal records, contact information, financial conditions, social activities and other information which may directly or indirectly be used to identify a living natural person.

Definition of sensitive personal data

According to PDPL, sensitive personal data means the personal data relating to medical treatments, genetic information, sex life, health checks and criminal records. As mentioned above, the provisions relating to sensitive personal data remain ineffective. At the moment, sensitive personal data will be treated like other data.

NATIONAL DATA PROTECTION AUTHORITY

In Taiwan, there is no single national data protection authority. The various ministries and city/county governments serve as the competent authorities.

REGISTRATION

Unlike the CPPL, there is no need to register with any authorities for the collection, processing, usage and international transfer of personal data under the PDPL.

DATA PROTECTION OFFICERS

There is no requirement in Taiwan for the data controller to appoint a data protection officer. However, if the data controller is a government agency, a specific person should be appointed to be in charge of the security maintenance measures.

COLLECTION & PROCESSING

Under the PDPL, the data controller should not collect or process personal data unless there is specific purpose and should comply with one of the following conditions:

- where collection/processing is explicitly stipulated by law
- where there is a contract or quasi contract between the data controller and the data subject
- where the data subject has him/herself disclosed such data or where the data has been publicised legally
- where it is necessary for public interest on statistics or the purpose of academic research conducted by a research institution. The data may not lead to the identification of a certain person after the treatment of the provider or by the disclosure of the collector
- where written consent has been given by the data subject
- where the public interest is involved, or
- where the personal data is obtained from publicly available sources, except that where the vital interest of the data subject requires more protection and the prohibition of the processing or usage of such personal information.

Furthermore, except for the exemptions stipulated in the PDPL (eg if it is explicitly stipulated by law that the provision of such information is not required), the data controller is permitted to collect and process personal data only if the data controller unambiguously informs the data subject of the following information prior to or upon the collection:

- data controller's name
- purpose for collecting personal data
- categories of personal data
- period, area, recipients and means of using the data
- the data subject's rights and the methods by which the data subject may exercise those rights in accordance with the PDPL, and
- where the the data subject has the right to choose whether or not to provide the data, the consequences of not providing the data.

The information collected should in principle only be used for the purpose notified and not for any other purpose.

In addition, the Employment Service Act and its Enforcement Rules require that an employer shall not request a job seeker or an employee to provide his privacy information which is unrelated to his employment. Such privacy information includes physiological information, psychological information and personal life information. When an employer asks a job seeker or an employee to provide his/her privacy information, the personal interest of the data subject should be respected; the request should not exceed necessary scope of specific purposes based on economic demand or public interest, and should have just and reasonable connection with the specific purposes.

TRANSFER

The central competent authority may restrict the international transfer of personal data by the data controller which is not

a government agency if:

- it involves major national interests
- where a national treaty or agreement specifies otherwise
- where the country receiving personal data lacks proper regulations that protect personal data and that might harm the rights and interests of the data subject, or
- where the international transfer of personal data is made to a third country through an indirect method in order to evade the provisions of the PDPL.

SECURITY

Data controllers which are non government agencies should adopt proper security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.

The central competent authority may request the data controller to set up a plan for the security measures of the personal data file or the disposal measures for the personal data after termination of business.

BREACH NOTIFICATION

Where the personal data is stolen, disclosed, altered or infringed in other ways due to the violation of the PDPL, the data controller should notify the data subject.

ENFORCEMENT

Under the PDPL, the competent authority may perform an inspection, if it is necessary for the protection of personal data, of the disposal measures after termination of business, the limitation of international transfer, other routine examinations, or if the PDPL may be violated. Those who perform the inspection may ask the data controller to provide a necessary explanation, take cooperative measures, or provide relevant evidence.

When the competent authority conducts such an inspection, it may seize or duplicate the personal data and files may be confiscated or may be used as evidence. The owner, holder or keeper of that data or those files should surrender them upon request.

In addition, a breach of the PDPL may be subject to criminal sanctions, administrative fines, and civil compensation (class action is permitted).

ELECTRONIC MARKETING

The PDPL applies to electronic marketing in the same way as to other marketing. Within the necessary scope of specific purposes of data collection, the data controller may use personal data for marketing. However, when the data subject refuses the marketing (a right to 'opt-out'), the data controller should cease using such personal data for marketing. In addition, when making the first marketing, the data controller should bear the costs to provide the data subject with the means to refuse marketing.

ONLINE PRIVACY

There is no special law or regulation applicable to online privacy. The PDPL applies to online and physical world in the same manner. As a result, online unique issues are not specifically addressed.

KEY CONTACTS

Formosa Transnational Attorneys at Law
www.taiwanlaw.com/

Chun-yih Cheng
Senior Partner
T +886 2 27557366 Ext 158
chun-yih.cheng@taiwanlaw.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

THAILAND

Last modified 28 January 2015

LAW IN THAILAND

At present, Thailand does not have any general statutory law governing data protection or privacy. However, the Constitution of the Kingdom of Thailand does recognize the protection of privacy rights. In addition, statutory laws in some specific areas (such as telecommunications, banking and financial businesses (Specific Businesses) as well as other non-business related laws, such as certain provisions under Thai Penal Code and the Child Protection Act B.E. 2543 (2003), do provide a certain level of protection against any unauthorised collection, processing, disclosure and transfer of personal data.

Recently, the draft Personal Information Protection Act ('Draft'), which has been reviewed by the Council of State, was given to the Committee for House of Representative Coordination to review and analyse if there are any practical issues on applying the law and how the Data Protection Committee should be formed.

The Draft is being reviewed by the Office of the Public Sector Development Commission and will be submitted to the Cabinet for approval later. The current Draft provides protection of personal data by restricting the gathering, using, disclosing and altering of any personal data without the consent of the data owner. The Draft also imposes both criminal penalties and civil liability for any violation of the Draft and calls for the establishment of a Protection of Personal Data Commission to regulate compliance with the Draft.

Notwithstanding the above, at present, no clear indication exists as to when the Draft will be final, or whether it will ultimately be enacted into binding law.

DEFINITIONS

Definition of personal data

According to the Draft, 'personal data' means any information or data relating to an identified natural person or that can identify a natural person by reference to the facts, data or any other materials about that natural person.

The information or data may be in the form of documents, files, reports, books, charts, portraits, photos, films, recorded images or sounds that may be kept or stored in computer machines or in any other means that can be used to make the recorded information or data seen. Personal Data shall also include facts about, or behaviours of, a deceased person.

Definition of sensitive personal data

Not available in the present Draft.

NATIONAL DATA PROTECTION AUTHORITY

None at present – see detail in 'Law' section above.

REGISTRATION

No registration requirement with respect to the collection or use of personal data exists.

DATA PROTECTION OFFICERS

No requirement exists in Thailand for an organisation to appoint a data protection officer.

COLLECTION & PROCESSING

Statutory laws provide a certain level of protection for the accumulation, retention and release of personal data for Specific Businesses.

For example, a telecommunications operator may collect personal data from customers only for the purpose of its business operation and as permissible by law. The collection of sensitive information, such as physical handicaps or genetics, is strictly prohibited. Operators must also have proper security measures in place to protect customers' data, including any of their personal data. Any release of personal data, except disclosure for national security purposes, requires the data owner's consent.

According to the Child Protection Act, the guardian of a child's safety or a child's safety protector are forbidden to disclose the name, surname, picture or any information regarding the child and the child's guardian in a manner which is likely to be detrimental to the reputation, esteem or entitlements of the child. This is also applied *mutatis mutandis* to a competent official, social worker, psychologist or person having the duty to protect a child's safety, who has come into the possession of such information as a result of the performance of his or her duties. It is also forbidden for any person to advertise or disseminate by means of the mass media or any other form of information technology the disclosed information in violation of the aforementioned provisions.

If no specific statutory law is applicable then generally, the collection and processing of personal data with the consent (preferably written) of the data owner is permissible.

TRANSFER

Under the Thai Civil and Commercial Code, a person who wilfully, negligently, or unlawfully injures the life, body, health, liberty, property or any right of another person has committed a wrongful act and is required to compensate the victim. Disclosure or transfer of data may be considered a wrongful act if it causes damage to the data owner.

In practice, the prior written consent of the data owner should be obtained before transferring the data to any third person. Disclosure of data without the consent of the data owner is permissible in very limited circumstances (eg pursuant to an order from a government authority or Thai court).

SECURITY

Data controllers in Specific Businesses are required to maintain an appropriate level of security to protect any stored personal data from unauthorised access. Failure to comply with this requirement normally results in both imprisonment and monetary penalties.

Data controllers in non-Specific Businesses are also recommended to implement appropriate security measures to protect personal data from unauthorised access. If unauthorised access causes any damage to the data owner, the data controller may also be liable under the Thai Civil and Commercial Code for committing a wrongful act by failing to prevent the unauthorised access.

BREACH NOTIFICATION

No notification requirement exists with respect to privacy or data protection law.

ENFORCEMENT

No organisation in Thailand is primarily responsible for the enforcement of privacy or data protection law.

ELECTRONIC MARKETING

Presently, there is no specific law that prohibits the use of personal data for the purposes of electronic marketing. The availability of option for opt-in and opt-out is just the practice as a norm and not yet the law.

ONLINE PRIVACY

At present, there is no provision under the relevant laws and the Draft that specifically prohibits or controls the placing of cookies on users' computers.

Although there are provisions under the Computer Crime Act B.E. 2550 (2007), imposing punishments for certain computer data alterations, the computer cookies or location tracing mechanisms are excluded as they will not cause any of the above alterations to happen to computers. Those below acts are punishable:

- any person who illegally damages, destroys, corrects, changes or amends a third party's computer data, either in whole or in part, shall be subject to imprisonment for no longer than 5 years or a fine of not more than THB 100,000, or both
- any person who illegally commits any act that causes the working of a third party's computer system to be suspended, delayed, hindered or disrupted to the extent that the computer system fails to operate normally shall be subject to imprisonment for no longer than 5 years or a fine of not more than THB 100,000, or both, and
- any person sending computer data or electronic mail to another person and covering up the source of such aforementioned data in a manner that disturbs the other person's normal operation of their computer system shall be subject to a fine of not more than THB 100,000.

KEY CONTACTS

Dr. Chanvitaya Suvarnapunya
Partner
T +662 686 8500
chanvitaya.suvarnapunya@dlapiper.com

Chadaporn Ruangtoowagoon
Senior Associate
T +662 686 8579
chadaporn.ruangtoowagoon@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

TRINIDAD AND TOBAGO

Last modified 28 January 2015

LAW IN TRINIDAD AND TOBAGO

In Trinidad and Tobago *The Data Protection Act, 2011* provides for the protection of personal privacy and information ('DPA') processed and collected by public bodies and private organisations.

The DPA was partially proclaimed on the 6th January 2012 by Legal Notice 2 of 2012 and only Part I and sections 7 to 18, 22, 23, 25(1), 26 and 28 of Part II have come into operation.

No timetable has been set for the proclamation of the remainder of the DPA and it is possible that there may be changes to the remainder of the legislation before it is proclaimed.

DEFINITIONS

Definition of personal data

Personal data (which is referred to in the DPA as 'Personal Information') is defined as information about an identifiable individual that is recorded in any form including:

- the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual
- the address and telephone number of the individual
- any identifying number, symbol or other particular identifier designed to identify the individual
- information relating to the individual's race, nationality or ethnic origin, religion, age or marital status
- information relating to the education or the medical, criminal or employment history of the individual, or information relating to the financial transactions in which the individual has been involved or which refer to the individual
- correspondence sent to an establishment by the individual
- information that is explicitly or implicitly of a private or confidential nature, and any replies to such correspondence that would reveal the contents of the original correspondence
- the views and opinions of any other person about the individual, and
- the fingerprints, DNA, blood type or other biometric characteristics of the individual.

Definition of sensitive personal data

Sensitive Personal Data (which is referred to in the DPA as 'sensitive personal information') is defined as personal information on a person's:

- racial or ethnic origins
- political affiliations or trade union membership
- religious beliefs or other beliefs of a similar nature
- physical or mental health or condition
- sexual orientation or sexual life, or
- criminal or financial record.

NATIONAL DATA PROTECTION AUTHORITY

The entity responsible for the oversight, interpretation and enforcement of the DPA is the Office of the Information Commissioner. It has broad authority, including to authorise the collection of personal information about an individual from third parties and to publish guidelines regarding compliance with the Act.

REGISTRATION

There is no registration requirement under the DPA.

DATA PROTECTION OFFICERS

There is no such requirement under the DPA.

COLLECTION & PROCESSING

The knowledge and consent of the individual is required for the collection, use and disclosure of personal information. Furthermore, collection is required to be undertaken in accordance with the purpose identified by the organisation collecting, the personal information and other legal requirements.

Sensitive personal information may not be processed except as specifically permitted by law.

The DPA includes provisions that relate specifically to the collection and processing of personal information by public bodies and private enterprises respectively, however these are not yet in force. Nevertheless, they are presented below.

Public Bodies

Part III of the DPA provides that a public body may collect and process personal data when the following conditions are met:

- the collection of that information is expressly authorised by law
- the information is collected for the purpose of law enforcement
- the information relates directly to and is necessary for an operating programme or activity of the public body
- the collection of personal information is collected directly from the individual:
    - another method of collection is authorised by the individual, Information Commissioner or law
    - the information is necessary for medical treatment
    - the information is required for determining the suitability of an award

- for judicial proceedings
- the information is required for the collection of a debt or fine, or
- it is required for law enforcement purposes

- the individual is informed of the purpose for collecting his/her personal information; the legal authorisation for collecting it and contact details of the official or employee of the public body who can answer the individual's questions about the collection.

Private Bodies

Part IV of the DPA provides that the collection and processing of personal information by private organisations will be in accordance with certain Codes of Conduct (which are to be determined by the Office of the Information Commissioner in consultation with the private sector) and with the General Privacy Principles (which are currently in force).

Sensitive Information

As to both public bodies and private organisations, Sensitive Personal Information may not be processed without the consent of the individual unless:

- it is necessary for the healthcare of the individual
- the individual has made the information public
- it is for research or statistical analysis
- it is by law enforcement
- for the purpose of determining access to social services, or
- as otherwise authorised by law.

TRANSFER

Section 6(1) of the DPA provides that personal information may be transferred outside of Trinidad and Tobago only if the foreign country requesting the individual's personal information has safeguards for the regulation of the personal information which are comparable to Trinidad and Tobago's.

In this regard, the Office of the Information Commissioner is required to publish in the *Gazette* and at least two newspapers in daily circulation in Trinidad and Tobago a list of countries which have comparable safeguards for personal information as provided by this Act. As of January 6, 2015, this has not yet happened because a Commissioner has yet to be appointed.

Sections 72(1) and (2) of the DPA (neither of which are in force as yet) provide that where a mandatory code is developed for private bodies it must require at a minimum that personal information under the custody or control of a private organisation not be disclosed to a third party without the consent of the individual to whom it relates, subject to certain conditions. Where personal information under the custody and control of an organisation is to be disclosed to a party residing in another jurisdiction, the organisation must inform the individual to whom the information relates.

Section 6 of the DPA, which is in force, states that all persons who handle, store or process personal information belonging to another person are subject to the following 'General Privacy Principles':

- an organisation shall be responsible for the personal information under its control
- the purpose for which personal information is collected shall be identified by the organisation before or at the time of collection
- knowledge and consent of the individual are required for the collection, use or disclosure of personal information

- collection of personal information shall be legally undertaken and be limited to what is necessary in accordance with the purpose identified by the organisation
- personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual
- personal information shall be accurate, complete and up-to-date, as is necessary for the purpose of collection
- personal information is to be protected by such appropriate safeguards having regard to the sensitivity of the information
- sensitive personal information is protected from processing except where specifically permitted by written law
- organisations are to make available to individuals documents regarding their policies and practices related to the management of personal information, except where otherwise provided by written law
- organisations shall, except where otherwise provided by written law, disclose at the request of the individual, all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information
- the individual has the ability to challenge the organisation's compliance with the above principles and receive timely and appropriate engagement from the organisation, and
- personal information which is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

SECURITY

The DPA generally requires that personal information be protected by appropriate safeguards based on the sensitivity of the information. Sensitive personal information may not be processed except where permitted by law.

BREACH NOTIFICATION

There is no provision in the DPA for notifying data subjects or the Information Commissioner of a security breach.

ENFORCEMENT

The Office of the Information Commissioner is responsible for monitoring the administration of this Act to ensure that its purposes are achieved (s.9 (1)).

The Information Commissioner has several broad powers to conduct audits and investigations of compliance with the DPA.

Part V of the DPA (which is not in force) details the penalties for contraventions of the DPA and also makes further provisions for the enforcement of the DPA.

ELECTRONIC MARKETING

The DPA has no specific provision regarding electronic marketing.

ONLINE PRIVACY

The DPA has no specific provision regarding online privacy.

KEY CONTACTS

M. Hamel Smith & Co.
www.trinidadlaw.com/

Jonathan Walker
Partner
T +1 868 821 5500 ext. 5625
jonathan@trinidadlaw.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

TURKEY

Last modified 8 July 2016

LAW IN TURKEY

In Turkey, the Law on Protection of Personal Data ("**The Law**") w. no. 6698 is the specific data protection legislation. The Law was accepted in the Turkish Parliament on March 24, 2016 and was published in the Official Gazette on April 07, 2016.

DEFINITIONS

Definition of personal data

In the Law, personal data was described as *"Any information relating to an identified or identifiable natural person"*.

Definition of sensitive personal data

Sensitive personal data (Special Categories of Personal Data as mentioned in the Law) is defined as *"…data revealing data subject's ethnicity, political views, philosophical beliefs, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, information related to health, sex life, previous criminal convictions and biometric data…"*

NATIONAL DATA PROTECTION AUTHORITY

Currently there is no independent body governing data protection in Turkey.

The new Law introduces two bodies to watch over and regulate data processing and transfer activities. These are; **a)** Data Protection Board and **b)** Data Protection Authority. Both of these bodies have not yet been established as of mid-2016 however the Law stipulates that these bodies will be established as of October 7, 2016.

The Data Protection Board will be an independent decision making body whereas Data Protection Authority will be operating under the Prime Ministry.

REGISTRATION

As of October 7, 2016, all data controllers are required to enlist with the Data Protection Registry to be held under the Data Protection Authority and under supervision of the Data Protection Board.

DATA PROTECTION OFFICERS

There is no requirement in Turkey to appoint a data protection officer.

COLLECTION & PROCESSING

Pursuant to the Law, it is mandatory to comply with certain principles to collect and process personal data. In light of such principles personal data must be;

- processed fairly and lawfully,
- accurate and up to date,
- processed for specific, explicit and legitimate purposes
- relevant, adequate and not excessive
- kept for a term necessary for purposes for which the data have been processed.

Further, in principle, personal data cannot be processed without being collected and processed with explicit consent of the data subject. However the Law stipulates certain exceptions where consent is not required. These are;.

- processing is expressly permitted in the law
- processing is necessary for protection of data subject's, who is not in a situation to give consent due to an actual impossibility or a person whose consent is not legally recognized, or third parties' life or physical integrity,
- processing personal data of contractual parties is necessary for forming or the performance of a contract
- processing is mandatory for the data controller to perform his/her legal obligation
- personal data has been opened to the public by data subject
- processing is mandatory for assigning, using or protecting a right.
- processing is mandatory for legitimate interest of data processor and without damaging rights of data subject.

As part of the collection of data from the data subject the controller is obliged to provide the data subject with the following information:

- the identity of the controller and of his representative, if any
- the purposes of the processing for which the data is intended
- the recipients of the data and the reasons for transfer
- the process of collecting data and the legal grounds, and
- the rights of the data subject.

Where the data has not been obtained from the data subject, the controller shall provide the data subject with the above stated information as well as details of the categories of data concerned.

Processing of sensitive personal data without explicit consent of the data subject is forbidden. However sensitive data other than health and sex life data can be processed without explicit consent of data subject only if a law/legislation permits such processing. Further, health data and sex life data can only be processed by natural persons who are under oath of secrecy or by authorities for the purposes of protecting public health, preventive medicine, medical diagnosis, the provision of care and treatment services or planning, management and financing of health-care services

TRANSFER

The Law distinguishes transfer of personal data to third parties in Turkey and transfer of personal data to third countries.

Transfer of personal data to third parties

In principle, personal data can be transferred to third parties with explicit consent of data subject. The conditions and exemptions applied to collection and processing of personal data are applied for transfer of personal data to third parties.

Transfer of personal data to parties in third countries

In addition to conditions and exemptions applied for transfer of personal data to third parties, either of the following conditions shall exist for transfer of data to parties in third countries;

a) the country to which personal data will be sent shall have sufficient level of protection

b) the data controller in Turkey and target country shall undertake protection in writing and obtain the Data Protection Board's permission.

SECURITY

In light of the provisions of the Law and consistent with the principles of good faith those entrusted with personal data are expected to ensure protection of such data. Under the Law, data controller is required to ensure that appropriate technical and organisational measures are taken to prevent all illegal processing and to ensure the data is not destroyed, lost, amended, disclosed or transferred without authority. Such measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected.

BREACH NOTIFICATION

There is no breach notification requirement; nonetheless, in the event that data is inadvertently or erroneously lost, transferred, destroyed etc., notification should be made to the data subjects in accordance with the principles of good faith. Furthermore, each situation should be evaluated in accordance with provisions of the applicable specific law, if any, as more strict procedures may apply.

ENFORCEMENT

The Law and the Turkish Criminal Code No. 5237 imposes custodial sentences for the unlawful processing of data. The Turkish Civil Law No. 4721 affords the right to claim compensation for the unjust use of data and a number of other laws impose administrative fines.

Furthermore, the Law introduces administrative fines up to TRY 1.000.000 (€ 315.000) for those who act against the requirements or rules in the Law.

ELECTRONIC MARKETING

The Law on Regulation of Electronic Trade has been published in the Official Gazette on 5 November 2014. The Law entered into force on 1 May 2015. Further, secondary legislation (The Regulation on Electronic Trade) was published in the Official Gazette on 26 August 2015 and entered into force on the same date.

Pursuant to the Law, commercial electronic communication (electronic marketing) can only be sent by obtaining prior consent (opt-in) from recipients. Such consent can be obtained in writing or through means of electronic communication. It is required that the commercial electronic communication is in compliance with the consent obtained from recipients. Further, the identity of the service provider, contact information (such as e-mail, sms, telephone number, fax number (depending on the type of commercial electronic communication) and if made on behalf of a third party information the third party must be present.

Pursuant to the Law, consumers have the right to refuse commercial electronic communication. The service provider is obliged to allow the free transmission of the refusal. Commercial electronic communications to recipient must be ceased within 3 business days from the receipt of refusal. Non-compliance with the above obligations stated is subject to administrative fines between 1.000 TRY to 15.000 TRY (approx. 350 - 5.350 EUR).

ONLINE PRIVACY

There is no specific law on online privacy with specific provisions on Cookies and Location Data. However, Law No. 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting enables internet users to initiate prosecution in case of infringements of their personal rights.

KEY CONTACTS

Burak Özdağıstanli
Senior Associate
T +90 212 318 05 16
bozdagistanli@yukselkarkinkucuk.av.tr

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

UAE - DUBAI (DIFC)

Last modified 21 March 2016

LAW IN UAE - DUBAI (DIFC)

Note: Please also see 'UAE – General'.

The DIFC implemented DIFC Law No. 1 of 2007 Data Protection Law in 2007 which was subsequently amended by DIFC Law No. 5 of 2012 Data Protection Law Amendment Law ('DPL').

In addition, under the powers granted to the Commissioner of Data Protection ('CDP') under Article 27 of the DPL, the CDP has issued the Data Protection Regulations ('DPR').

DEFINITIONS

Definition of Personal Data

Any data referring to an Identifiable Natural Person

Definition of Identifiable Natural Person

Is a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.

Definition of Sensitive Personal Data

Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life.

Definition of Process, Processed, Processes and Processing

Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

NATIONAL DATA PROTECTION AUTHORITY

The Commissioner of Data Protection ('CDP') is essentially the regulating body in the DIFC.

The Data Protection Commissioner

Dubai International Financial Centre Authority
Level 14, The Gate
P.O. Box 74777
Dubai
United Arab Emirates

administrator@dp.difc.ae

Tel: +971 4 362 2623
Fax: +971 4 362 2656

REGISTRATION

Unless certain exceptions apply, Data Controllers must obtain a permit from the CDP prior to commencing a Processing Operation involving either Sensitive Personal Data or transferring Personal Data outside of the DIFC.

Data Controllers must also notify the CDP of any Processing operations involving either Sensitive Personal Data or the transfer of Personal Data outside of the DIFC.

DATA PROTECTION OFFICERS

There is no requirement under the DPL or the DPR, for organisations to appoint a data protection officer, though note the general obligation of a Data Controller to implement appropriate technical and organisational measures to protect Personal Data, as further detailed below (see separate **Security** section).

COLLECTION & PROCESSING

Data Controllers may collect and process Personal Data when any of the following conditions are met:

- the Data Subject has given his/her written consent to the Processing of that Personal Data (DPL, Article 9(a))
- processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract (DPL, Article 9(b))
- processing is necessary for compliance with any legal obligation to which the Data Controller is subject (DPL, Article 9(c))
- processing is necessary for the performance of a task carried out in the interests of the DIFC, or in the exercise of the DIFC Authority, the Dubai Financial Services Authority, the Court and the Registrar's functions or powers vested in the Data Controller or in a third party to whom the Personal Data are disclosed (DPL, Article 9(d)), or
- processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by the third party or parties to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation (DPL, Article 9(1)(e)).

Data Controllers may collect and process Sensitive Personal Data when any of the following conditions are met:

- the Data Subject has given his/her written consent to the Processing of that Sensitive Personal Data (DPL, Article 10(1)(a))
- processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller (DPL, Article 10(1)(b))
- 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 consent (DPL, Article 10(1)(c))

- processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed to a Third Party without the consent of the Data Subjects (DPL, Article 10(1)(d))

- the Processing relates to Personal Data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defence of legal claims (DPL, Article 10(1)(e))

- processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject (DPL, Article 10(1)(f))

- processing is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation (DPL, Article 10(1)(g))

- processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that apply to a Data Controller (DPL, Article 10(1)(h))

- processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Personal Data is Processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (DPL, Article 10(1)(i))

- processing is required for protecting members of the public against dishonesty, malpractice or other seriously improper, or any resultant financial loss (DPL, Article 10(1)(j)), or

- authorised in writing by the CDP (DPL, Article 10(1)(k)).

TRANSFER

Data Controllers may transfer Personal Data out of the DIFC if the Personal Data is being transferred to a Recipient in a jurisdiction that has laws that ensure an adequate level of protection for that Personal Data (DPL, Article 11(1)(a)). An adequate level of protection is when the level of protection in that jurisdiction is acceptable pursuant to the DPR or any other jurisdiction approved by the CDP (DPL, Article 11(2)).

In the absence of an adequate level of protection, Data Controllers may transfer Personal Data out of the DIFC if the:

- CDP has granted a permit or written authorisation for the transfer or the set of transfers and the Data Controller applies adequate safeguards with respect to the protection of this Personal Data (DPL Article 12(1)(a)). Article 5.1 of the DPR then sets out the requirements for applying for such a permit (including a description of the proposed transfer of Personal Data for which the permit is being sought and including a description of the nature of the Personal Data involved)

- data Subject has given his/her written consent to the proposed transfer (DPL, Article 12(1)(b))

- transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request (DPL, Article 12(1)(c))

- transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a third party (DPL, Article 12.1(d))
- transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defence of legal claims (DPL, Article 12.1(e))
- transfer is necessary in order to protect the vital interests of the Data Subject (DPL, Article 12.1(f))
- transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case (DPL, Article 12(1)(g))
- transfer is necessary for compliance with any legal obligation to which the Data Controller is subject or the transfer is made at the request of a regulator, police or other government agency (DPL, Article 12(1)(h))
- transfer is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by legitimate interests of the Data Subject relating to the Data Subject's particular situation (DPL, Article 12(1)(i)), or
- transfer is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that applies to a Data Controller (DPL, Article 12(1)(j)).

Authorities who may receive Personal Data in the context of a particular inquiry are not regarded as Recipients under the DPL or the DPRs (as per the definition of Recipient in the DPL).

Safe Harbor Ruling - October 2015

On 26 October 2015 the CDP issued a guidance to DIFC registered entities regarding the adequacy status of US Safe Harbor recipients.

The guidance was issued as a result of a decision by the European Court of Justice (ECJ) on 6 October 2015 which invalidated the European Commission's Decision 200/520/EC. That EC Decision had provided "adequate protection status" for personal data transfers from European Member States to US Safe Harbor recipients.

As noted above, DPL, Article 11 allows a transfer of personal data out of the DIFC if:

1. an adequate level of protection for that personal data is ensured by the laws and regulations that are applicable to the recipient; or
2. in accordance with DPL, Article 12.

Like the European Commission, the DIFC Data Commissioner had previously listed the US Safe Harbor scheme as a jurisdiction with an "adequate level of protection" on its website. The US Safe Harbor scheme has however now been removed from that list.

The DIFC Data Commissioner's guidance observes that, as the DIFC Data Protection Laws are largely modelled on relevant EU Directives, the ECJ decision has caused the DIFC Data Commissioner to reconsider the adequacy status previously provided to US Safe Harbor rules. It has noted however that there are currently ongoing negotiations between EU and US authorities regarding the framework.

In light of the above, the DIFC Data Commissioner warns that DIFC organisations should continue to protect individuals' personal data when transferred to the US and consider potential risks by implementing appropriate legal and technical

solutions in a timely manner. DIFC entities transferring personal data to the US should rely upon the conditions referred to in DPL, Article 12 until further clarity is provided.

It is expected that the CDP will release further guidance on how DIFC entities should navigate the Data Protection Law to enable them to legally transfer personal data to the US in the near future.

SECURITY

Data Controllers must implement appropriate technical and organisational measures to protect Personal Data against wilful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, in particular where Sensitive Personal Data is being Processed or where the Personal Data is being transferred out of the DIFC (DPL, Article 16(1)). When applying for a permit to Process Sensitive Personal Data, or Transfer Personal Data out of the DIFC, Data Controllers must include detail regarding the safeguards employed to ensure the security of such Sensitive Personal Data/Personal Data (respectively, Articles 2.1.1(i) and 5.1.1(i) of the DPR).

The measures implemented ought to ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected (DPL, Article 16(2)).

BREACH NOTIFICATION

In the event of a breach (being an unauthorised intrusion, either physical, electronic or otherwise, to any Personal Data database, as defined by the DPL) Data Controllers (or Data Processors carrying out a Data Controller's function at the time of the breach), must inform the CDP of the incident as soon as reasonably practicable (DPL, Article 16(4)).

ENFORCEMENT

In the DIFC, the CDP oversees the enforcement of the DPL (DPL, Article 26).

The CDP needs to conduct all reasonable and necessary inspections and investigations before notifying a Data Controller that it has breached or is breaching the DPL or any regulations (DPL, Article 33). If the CDP is satisfied with the evidence of the breach, the CDP may issue a direction to the Data Controller requiring it to do either or both of the following:

- do or refrain from doing any act or thing within such time as may be specified in the direction (DPL, Article 33(1)(a)), or
- refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction (DPL, Article 33(1)(b)).

A Data Controller may ask the CDP to review the direction within fourteen days of receiving a direction and the CDP may receive further submissions and amend or discontinue the direction (DPL, Article 33(6)).

A Data Controller that fails to comply with a direction of the CDP may be subject to fines and liable for payment of compensation (DPL, Article 33(4)).

In addition, if the CDP considers that a Data Controller or any officer of it has failed to comply with a direction, he may apply to the Court for one or more of the following orders:

- an order directing the Data Controller or officer to comply with the direction or any provision of the Law or the Regulations or of any legislation administered by the CDP relevant to the issue of the direction (DPL, Article 33(5)(a))
- an order directing the Data Controller or officer to pay any costs incurred by the CDP or other person relating to the issue of the direction by the CDP or the contravention of such Law, Regulations or legislation relevant to the

issue of the direction (DPL, Article 33(5)(b)), or

- any other order that the Court considers appropriate (DPL, Article 33(5)(c)).

Any Data Controller who is found to contravene the DPL or a direction of the CDP may appeal to the DIFC Court within 30 days (DPL, Article 37(1)). The DIFC Court may make any orders that it thinks just and appropriate in the circumstances, including remedies for damages, penalties or compensation (DPL, Article 37(2)).

ELECTRONIC MARKETING

As soon as possible upon beginning to collect Personal Data, the DPL requires Data Controllers to provide Data Subjects who they have collected Personal Data from, with, amongst other things, any further information to the extent necessary (having regard to the specific circumstances in which the Personal Data is collected). This includes information on whether the Personal Data will be used for direct marketing purposes (DPL, Article 13).

If the Personal Data has *not* been obtained from the Data Subject, the Data Controller or their representative must at the time of undertaking the Processing – or if it is envisaged that the Personal Data will be disclosed to a Third Party, no later than when the Personal Data is first Processed or disclosed – provide the Data Subject with, amongst other things, information regarding whether the Personal Data will be used for direct marketing purposes (DPL, Article 14).

Before Personal Data is disclosed for the first time to third parties or used on a Data Subject's behalf for the purposes of direct marketing, Data Subjects also have the right to be informed and to be expressly offered the right to object to such disclosures or uses (DPL, Article 18).

Additionally, the DPL requires a Data Controller to record various types of information regarding its Personal Data Processing operations (Article 19(4)). This must include an explanation of the purpose for the Personal Data Processing (DPL, Article 6.1.1(b)). The DPR suggests that one of these purposes may be for advertising, marketing and public relations for the Data Controller itself or for others (Article 6.2.1).

ONLINE PRIVACY

The DPL or DPR do not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as UAE criminal law applies in the DIFC, the privacy principles laid out therein may apply (see **UAE - General** section).

KEY CONTACTS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Eamon Holley
Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com

Jamie Ryder
Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

Robert Flaws
Senior Legal Consultant
T +971 4 438 6287
robert.flaws@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

UAE - GENERAL

Last modified 21 March 2016

LAW IN UAE - GENERAL

Note: Please also see 'UAE – Dubai (DIFC)'.

In December 2015 the Dubai Government published the Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai, ("Dubai Data Law"). The purpose of the Dubai Data Law to collate and manage data that relates to the emirate of Dubai and, where appropriate, to publish it as Open Data or at least ensure that it is shared it between authorised persons. This law is considered unique as it is the only one in the world we are aware of that provides a government with the power to require designated private sector entities to provide to a government with information held by the company in relation to a city, for the purposes of making that information Open Data.

In addition, there are several UAE Federal Laws that contain various provisions in relation to privacy and the protection of personal data:

- Constitution of the UAE (Federal Law 1 of 1971)
- Penal Code (Federal Law 3 of 1987 as amended)
- Cyber Crime Law (Federal Law 5 of 2012 regarding Information Technology Crime Control), and
- Regulating Telecommunications (Federal Law by Decree 3 of 2003 as amended), which includes several implementing regulations/policies enacted by the Telecoms Regulatory Authority ('TRA') in respect of data protection of telecoms consumers in the UAE.

DEFINITIONS

The concept of 'Personal Data', as understood in the EU, is not reflected under UAE Federal Law. The corresponding concept within UAE Law encompasses notions such as 'secrets', 'photographs', 'the privacy of the individual or family life' and 'private life or family life secrets of individuals'. As such, while no UAE Federal Law explicitly states that the collection of personal data requires express consent, if any such data pertains to private or family life then, in certain circumstances, the consent of the individual(s) concerned may be required.

The term 'Personal Data' as used below refers to the UAE understanding of the concept as described above.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in the UAE. In respect of telecommunications services, the TRA is responsible for overseeing the relevant telecoms laws and policies.

REGISTRATION

There are no data protection registration requirements in the UAE.

DATA PROTECTION OFFICERS

There is no requirement in the UAE for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

If the collection and processing of any personal data pertains to an individual's private or family life then the consent of the individual may be required in certain circumstances. A failure to obtain such consent would constitute a breach of the Penal Code (Article 378) and could also be a breach of the:

- Cyber Crime Law if the personal data is obtained or processed through the internet or electronic devices in general (Articles 21 and 22), and
- Telecoms Law to the extent that data is obtained through any means of telecommunication, including through a telecommunications service provider, or any other electronic means. In addition, the facility should be made available for such consent to be withdrawn at a later stage (TRA Consumer Protection Regulations, Article 12.5).

The Cyber Crime Law criminalises obtaining, possessing , modifying, destroying or disclosing (without authorisation) electronic documents or electronic information relating to medical records (Article 7). Additionally, unlawful access via the internet or electronic devices of financial information (eg Credit Cards and Bank Accounts) without permission is an offence under Articles 12 and 13.

TRANSFER

According to the Penal Code (Article 379), personal data may be transferred to third parties inside and/or outside of the UAE if the data subjects have consented in writing to such transfer.

In addition, in circumstances where telecommunications service providers provide subscriber information to affiliates or third parties directly involved in the supply of the services requested by a subscriber, the third parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the information, and use such information only as needed for the provision of the requested services. Telecommunications service providers are required to ensure that the contracts between them and any affiliate or third party holds the other party responsible for the privacy and protection of the subscriber's information (TRA Consumer Protection Regulations, Article 12.8).

However, the requirement to obtain written consent may be waived, pursuant to the Penal Code (Article 377), where the personal data pertains to a crime to which the data subject is answerable and it is disclosed in good faith to the relevant authorities.

SECURITY

There are no specific provisions under UAE Federal Law relating to the type of measures to be taken or level of security to have in place against the unauthorised disclosure of personal data. Instead, the Cyber Crime Law focuses on offences related to accessing data without permission and/or illegally (Articles 2 and 3 of the Cyber Crime Law), including financial information (eg credit card information or bank account information) (Articles 12 and 13).

Article 12.1 of the TRA Consumer Protection Regulations requires telecommunications service providers to 'take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of subscriber information'. Article 12.3 further stipulates that telecommunications service providers must take 'all reasonable

measures to protect the privacy of Subscriber Information that it maintains in its files, whether electronic or paper form', and that 'reliable security measures' should be employed.

Based on the above, best practice from a UAE law perspective would be to take appropriate technical security measures against unauthorised or unlawful processing of, and against accidental disclosure of, personal data. The measures taken must ensure a level of security adequate enough to minimise the risk of liability arising out of a claim for breach of privacy made by a data subject.

BREACH NOTIFICATION

In principle, there is no mandatory requirement under UAE Federal Law to report data security breaches.

Data subjects based in the UAE, however, may be entitled to hold the entities in possession of their data, liable under the principles of the UAE Civil Code for their negligence in taking proper security measures to prevent the breach, if such breach has resulted in actual losses being suffered by the data subjects.

In relation to telecommunication services, the Telecoms Law and most Policies do not include an explicit requirement on service providers to take the initiative in notifying the TRA of a breach or alleged breach, unless a subscriber complains to a service provider about the unauthorised disclosure of his or her personal data. Such a notification would be included in the monthly reporting which is submitted to the TRA (Article 14.10.2 of the TRA Consumer Protection Regulations).

Subscribers are also able to complain directly to the TRA about the unauthorised disclosure of their personal data. However, the TRA will generally only handle subscriber complaints after the complaint has been submitted to the service provider and if the matter has not been satisfactorily resolved by the service provider's own customer complaints procedure (Article 14.11.1 of the TRA Consumer Protection Regulations and Article 1.1 to 1.3 of the TRA Consumer Dispute Procedure).

ENFORCEMENT

There are three possible methods of enforcement from a UAE law perspective:

1. Where the unauthorised disclosure of personal data results in a breach of the Penal Code:

The Public Prosecutor in either the Emirate:

- where the party suspected of the breach (‘Offender’) resides
- where the disclosure occurred

will have jurisdiction over a data subject’s complaint.

If after concluding investigations with the police, the Public Prosecutor is satisfied with the evidence compiled, charges may be brought against the suspect.

The case would then be transferred to the Criminal Courts of First Instance. The data subject may attach a civil claim to the criminal proceedings before the Courts have ruled on the case.

Pursuant to the Penal Code (Article 379), if the Courts find a suspect guilty of disclosing secrets that were entrusted to him 'by reason of his profession, craft, situation or art' the penalties to be imposed under the Penal Code may include a fine of at least UAE Dirhams 20,000 (the fine is determined by the Courts) and/or an imprisonment for at least one year. More generally, pursuant to the Penal Code (Article 378), 'a punishment of confinement and fine shall be inflicted on any person who attacks the sanctity of individuals' private or family life' by committing any of the acts described under Article 378 'other than the legally permitted cases or without the victim's consent'.

When ruling on the criminal case, the Criminal Courts would usually transfer a civil claim made by the data subject to

the Civil Courts of First Instance for further consideration. The data subject would need to prove the losses he/she has suffered as a direct result of the disclosure of his/her personal data before the Civil Courts in order for damages to be awarded.

2. Where the unauthorised disclosure of personal data results in a breach of the Cyber Crime Law:

The police in each Emirate have developed specialised cybercrime units to handle complaints that relate to breaches of the Cyber Crime Law.

As above, the cybercrime unit in the Emirate where:

- the Offender resides, or
- where the disclosure occurred

will have jurisdiction over a data subject's complaint.

The cybercrime unit would investigate the case and decide whether or not to refer it to the Public Prosecutor in the same Emirate. If the case is referred and the Public Prosecutor is satisfied with the findings of the cybercrime unit, charges would be brought against the suspect. The same procedure identified above is then followed before the Courts.

If found guilty of an offence under the Cyber Crime Law, the punishment an Offender can receive varies depending on the nature of the crime. Punishments range from temporary detention, a minimum prison sentence of between six months or one year and/or a fine between AED 150,000 and 1,000,000 (Articles 2, 3, 7, 21 and 22 of the Cyber Crime Law). If found guilty of an attempt to commit any of the relevant offences under the Cyber Crime Law, the punishment is half the penalty prescribed for the full crime (Article 40).

3. Where the unauthorised disclosure of personal data results in a breach of the Telecoms Law and Policies:

The TRA is responsible for overseeing the enforcement of the Telecoms Law and in this regard may rely on the Police and Public Prosecutor in the Emirate where, either:

- the breach has occurred, or
- where the suspect resides.

Where a licensed telecommunications service provider has breached the law, the subscriber/data subject generally needs to complain first to the service provider about the breach, though a direct approach to the TRA may be accepted by the them at their discretion (Article 14.11.1 of the TRA Consumer Protection Regulations).

The subscriber's complaint needs to be submitted to the TRA within three months of the date when the service provider last took action . This three months requirement may be waived subject to the discretion of the TRA (Article 14.11.1 of the TRA Consumer Protection Regulations).

After examining the complaint the TRA may direct the service provider 'to undertake any remedy deemed reasonable and appropriate' (Article 14.11.5 of the TRA Consumer Protection Regulations).

ELECTRONIC MARKETING

No express laws are outlined under UAE law covering electronic marketing. However, Articles 21 and 22 of the Cyber Crime Law and Clause 3 of the Privacy of Consumer Information Policy, as described in the 'Collection and Processing' section above, are worded widely enough to potentially apply to electronic marketing. Article 22 of the Cyber Crime Law, for example, prohibits the use of various electronic devices in order to disclose, without permission, confidential information that has been obtained through the course of a person's duties.

ONLINE PRIVACY

Although the UAE Penal Code does not contain provisions directly relating to the internet, its provisions related to privacy are broadly drafted and therefore could apply to online matters (such as Article 378 as described above).

Additionally, as described in the 'Collection and Processing' section above, under certain circumstances, online privacy is protected through Articles 21 and 22 of the Cyber Crime Law and Clause 3 of the Privacy of Consumer Information Policy. Unlawful access via the internet, by electronic devices, of financial information (eg Credit Cards and Bank Accounts) without permission is also an offence under the Cyber Crime Law (Articles 12 and 13).

KEY CONTACTS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Eamon Holley
Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com

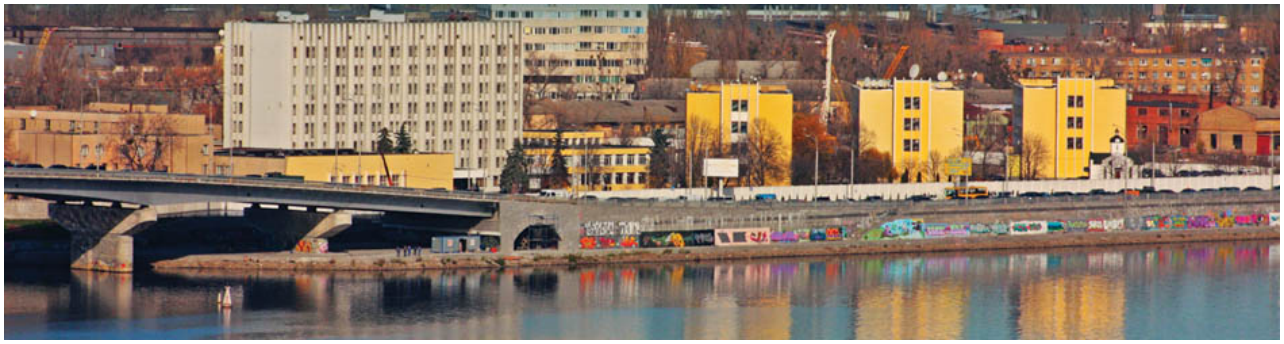
Jamie Ryder
Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

Robert Flaws
Senior Legal Consultant
T +971 4 438 6287
robert.flaws@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

UKRAINE



Last modified 27 January 2016

LAW IN UKRAINE

The Law of Ukraine No. 2297 VI 'On Personal Data Protection' as of 1 June 2010 (Data Protection Law) is the main legislative act regulating relations in the sphere of personal data protection in Ukraine. At 20 December 2012 Data Protection Law has been substantially amended by the Law of Ukraine 'On introducing amendments to the Law of Ukraine "On personal data protection' dated 20 November 2012 No. 5491-VI. Additional significant changes to Data Protection Law were envisaged by the Law of Ukraine 'On Amendments to Certain Laws of Ukraine regarding Improvement of Personal Data Protection System' dated 3 July 2013 No. 383-VII which came into force on 1 January 2014.

In addition to the Data Protection Law, certain data protection issues are regulated by subordinate legislation specifically developed to implement the Data Protection Law, in particular:

- Procedure of notification of the Ukrainian Parliament's Commissioner for Human Rights on the processing of personal data, which is of particular risk to the rights and freedoms of personal data subjects, on the structural unit or responsible person that organizes the work related to protection of personal data during processing thereof (Notification Procedure)
- Model Procedure of processing of personal data (Model Procedure)
- Procedure of control by the Ukrainian Parliament's Commissioner for Human Rights over the adherence of personal data protection legislation.

The Data Protection Law essentially complies with EU Data Protection Directive 95/46/EC.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, executed in Strasbourg at 28 January 1981 and the Additional Protocol to the Convention regarding supervisory authorities and trans border data flows, executed in Strasbourg at 8 November 2001 have also been ratified by Ukrainian Parliament at of 6 July 2010 (Convention on Automatic Processing of Personal Data) and thus fully effective in Ukraine.

Besides, the general data protection issues are regulated by:

- the Constitution of Ukraine dated 28 June 1996
- the Civil Code of Ukraine dated 16 January 2003 No 435 IV
- the Law of Ukraine 'On Information' dated 2 October 1992 No 2657 XII
- Law of Ukraine 'On Protection of Information in the Information and Telecommunication Systems' dated 5 July 1994 No. 80/94 VR
- the Law of Ukraine "On Electronic Commerce" dated 3 September 2015 No 675-VIII; and

- some other legislative acts.

DEFINITIONS

Definition of personal data

Data Protection Law defines 'personal data' as data or an aggregation of data on an individual who is identified or can be precisely identified.

Definition of sensitive personal data

There is no definition of 'sensitive personal data' as such envisaged by Ukrainian legislation.

At the same time, there is general prohibition to process personal data with regard to racial or ethnic origin, political, religious ideological convictions, participation in political parties and trade unions, accusation in criminal offences or conviction to criminal punishment as well as data relating to health or sex life of an individual.

Processing of the listed data is allowed if an unambiguous consent has been given by the personal data subject or based on exemptions envisaged by Data Protection Law (eg the processing is performed for the reasons of protection of vital interest of individuals, healthcare purposes, in course of criminal proceedings, anti-terrorism purposes, etc.).

NATIONAL DATA PROTECTION AUTHORITY

Starting from 1 January 2014 Ukrainian Parliament's Commissioner for Human Rights (Ombudsman) is the state authority in charge of controlling the compliance with the data protection legislation.

REGISTRATION

Starting from 1 January 2014 requirement of obligatory registration of personal data databases has been abolished. However according to new wording of Data Protection Law personal data owners are obliged to notify the Ombudsman about personal data processing which is of particular risk to the rights and freedoms of personal data subjects within thirty working days from commencement of such processing. Pursuant to the Notification Procedure, the following types of personal data processing requires obligatory notification of the Ombudsman processing of personal data on:

- racial, ethnic, national origin
- political, religious ideological convictions
- participation in political parties and/or organisations, trade unions, religious organisations or civic organisation of ideological direction
- state of health
- sexual life
- biometric data
- genetic data, and
- conviction to criminal or administrative liability
    - taking with regards to an individual interim injunction measures
    - taking with regards to an individual of measures stipulated by the Law of Ukraine 'On investigative activities'
    - taking with regards to an individual of certain types of violence; and
    - location and/or route of an individual.

The Notification Procedure envisages that the application for notification shall contain, inter alia the following information:

- information about the owner of personal data
- information about the processor(s) of personal data
- information on the composition of personal data being processed

- the purpose of personal data processing
- category(ies) of individuals whose personal data are being processed
- information on third parties to whom the personal data are transferred
- information on cross-border transfers of personal data
- information on the place (address) of processing of personal data, and
- general description of technical and organisational measures taken by personal data owned in order to maintain the security of personal data.

Where any of information listed above is submitted to the Ombudsman and has been changed, the owner of the personal data shall notify the Ombudsman on such changes within 10 days from the occurrence of such change.

Additionally, the Notification Procedure requires the owners of personal data to notify the Ombudsman on termination of personal data processing which is of particular risk to the rights and freedoms of personal data subjects within 10 days from the moment of such termination.

Furthermore, the Notification Procedure obliges the owners and processors of personal data processing the personal data which is of particular risk to the rights and freedoms of personal data subjects to notify the Ombudsman on establishing a structural unit or appointing a person (data protection officer) responsible for the organisation of work related to the protection of personal data during the processing thereof. Such notification shall be made within 30 days from the moment of establishing a structural unit or appointing a responsible person.

Information regarding the said notifications of the Ombudsman shall be published on the official website of the Ombudsman.

DATA PROTECTION OFFICERS

Legal entities shall establish a special department or appoint a responsible person (data protection officer) to organise the work related to the protection of personal data during the processing thereof.

There are no requirements for the Data Protection Officer to be a citizen or a resident in Ukraine. However, if he or she is a foreign citizen under the general rule a work permit must be obtained for him or her to hold such position. There are no particular penalties for incorrect appointment of Data Protection Officer.

COLLECTION & PROCESSING

The Data Protection Law provides for a requirement of obtaining the consent of personal data subjects on processing their personal data. According to the Data Protection Law the consent of personal data subject shall mean voluntary expression of will of the individual (subject to his/her awareness) to permit the processing of personal data for the determined purposes, expressed in writing or in some other form which allows the owner or processor of the personal data to make a conclusion that a consent has been granted. In the area of e-commerce, consent regarding processing of personal data may be granted in the process of registration of data subjects by "ticking" the respective box for giving consent on processing of their personal data for the determined processing purposes, provided that such a system does not allow processing of personal data before the consent from the data subject. In some instances provided by Data Protection Law (eg legislative permission for processing of personal data, conclusion and execution of a transaction in favour of the personal data subject, protection of interests of the subject or owner of personal data) personal data of individuals may be processed without the consent.

Pursuant to the Data Protection Law, as a general rule personal data subjects shall be informed, at the moment of collection of their personal data, of:

- the owner of their personal data
- composition and content of their personal data being collected
- their rights
- purpose of their personal data collection, and
- the persons to whom their personal data will be transferred.

However, in cases when the personal data of individuals have been collected based on the following grounds, the personal data subjects shall be informed of the above within 10 working days from the moment of their personal data's collection:

- legislative permission of the owner of personal data on processing of personal data exclusively for the purposes of fulfilling its authorities
- conclusion and execution of a transaction, in which the subject of personal data is a party or which has been concluded in favour of the subject of personal data or for taking actions, which preceded conclusion of a transaction at the request of the subject of personal data
- protection of vital interests of the subject of personal data, or
- need to protect legitimate interests of the owner of personal data, third parties, except where a subject of personal data demands to stop the processing of his/her personal data and the need in protection of personal data prevails over such interest.

In addition, the Data Protection Law provides the subject of personal data with the following rights:

- to be aware of the sources of collection, location of his/her personal data, the purpose of data processing, the address of the owner or processor of the personal data or to obtain the said information through his/her representatives
- to obtain information as regards the conditions of providing access to personal data, in particular, information on third parties, to which his/her personal data are transferred
- to access his/her personal data
- to obtain a reply within 30 calendar days from the date of receipt of his/her request, informing the individual whether his/her personal data are being processed and to receive the contents of such personal data
- to provide the owner of personal data with the reasonable request to terminate processing of his/her personal data
- to provide a reasonable request to change or destroy his/her personal data by any owner and processor of the personal data if the data is processed illegally or is inaccurate
- to protect of his/her personal data from unauthorised processing and accidental loss, elimination or damage with respect to intended encapsulation, not providing or the untimely providing of personal data, and also to protection from providing invalid or discrediting information regarding the individual
- to appeal violations in the course of personal data processing to the Ombudsman or to the court
- to introduce limitations as regards rights on its personal data processing while giving the consent
- to use the means of legal protection in the case of violation of rights to personal data
- to revoke its consent on personal data processing
- to be aware of the mechanism of automatic processing of personal data, and
- to be protected from the automated decision that has legal effect on it.

The owner of the personal data can entrust the processing of personal data to the processor of personal data under the written agreement between them. In this case the processor of personal data may process the personal data only for the purposes and in the volume provided by such agreement. The transfer of personal data to the processor of personal data can be allowed only by respective consent of the personal data subject.

TRANSFER

In accordance with Data Protection Law the personal data may be transferred to foreign counterparties only on condition of ensuring an appropriate level of protection of personal data by the respective state of the transferee. Pursuant to the Data Protection Law, such states include member-states of the European Economic Area and signatories to the EC Convention on Automatic Processing of Personal Data. The list of the states ensuring an appropriate level of protection of personal data will be determined by the Cabinet of Ministers of Ukraine.

Personal data may be transferred abroad based on one of the following grounds:

- unambiguous consent of the personal data subject
- cross-border transfer is needed to enter into or perform a contract between the personal data owner and a third party in favour of the personal data subject
- necessity to protect the vital interests of the personal data subjects
- necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement, or
- appropriate guarantees of the personal data owner as regards non-interference in personal and family life of the personal data subject.

SECURITY

The subjects of personal data relations are obliged to take appropriate technical and organisational measures to ensure the protection of personal data against unlawful processing, including against loss, unlawful or accidental elimination, and also against unauthorised access. In this regard, any owner of personal data shall determine a special department or a responsible person to organise the work related to the protection of personal data during the processing thereof.

The Model Procedure stipulates that the owners and processors of personal data shall take measures to maintain security of personal data on all stages of their processing including organisational and technical measures for the protection of personal data. Organisational measures shall include:

- determination of a procedure of access to personal data by employees of the owner/processor of personal data
- determine the order of recording of operations related to the processing of personal data of the subject and access to them
- elaboration of an action plan in case of unauthorised access to personal data, damage of technical equipment or occurrence of emergency situations, and
- regular trainings of employees which are working with personal data.

Personal data irrespective of the manner of its storage shall be processed in the way which makes unauthorised access to the data by third persons impossible.

With the purpose of maintenance of security of personal data, technical security measures shall be taken which would exclude the possibility of unauthorised access to personal data being processed and ensure proper work of technical and program complex through which the processing of personal data is performed.

Additionally, the Data Protection Law requires establishing a structural unit or appointing a responsible person within the personal data owners/processors processing the personal data which is of particular risk to the rights and freedoms of personal data subjects. Such structural unit or responsible person shall organize the work related to protection of personal data during the processing thereof.

BREACH NOTIFICATION

There is no requirement to report data security breaches or losses to the appropriate state authority.

ENFORCEMENT

According to Data Protection Law, the Ombudsman and Ukrainian courts are the state authorities responsible for controlling the compliance with personal data protection legislation. Failure to comply with the provisions of Data Protection Law can lead to responsibility prescribed by law.
Violation of personal data protection legislation may result in civil, criminal and administrative liability.

If the violation has led to material or moral damages, the violator can be obliged by the court to reimburse such damages.

The Code of Ukraine on Administrative Offenses envisages administrative liability for the following breaches of Ukrainian data protection legislation:

- failure to notify or delay in providing notification to the Ombudsman on the processing of personal data or on a change of information submitted which is subject to notification under Ukrainian legislation, or submission of incomplete or false information may lead to a fine of up to EUR 270
- non-fulfilment of legitimate requests (orders) of the Ombudsman or determined state officials of the Ombudsman's secretariat as regards the elimination or prevention of violations of personal data protection legislation may lead to a fine of up to EUR 671
- non-fulfilment of legitimate requests of Ombudsman or its representatives may lead to a fine of up to EUR 145
- non-observance of the established procedure for the protection of personal data which leads to unauthorised access to the personal data or violation of rights of the personal data subject may lead to a fine of up to EUR 671.

The criminal liability, prescribed by the Criminal Code of Ukraine envisages fines of up to EUR 671 or correctional works for a term of up to two years, or up to six months arrest, or up to three years of limitation of freedom for the illegal collection, storing, use, elimination, or spreading of confidential information about an individual, or an illegal change of such information.

ELECTRONIC MARKETING

The Law of Ukraine "On Electronic Commerce" dated 3 September 2015 provides for certain legal requirements for distribution of commercial electronic messages in the area of electronic commerce. In particular, commercial electronic messages shall be distributed only subject to the consent given by individual to whom such messages are addressed. At the same time, commercial electronic messages may be distributed to an individual without his/her consent only if such individual has an option to refuse from receiving of such messages in future.

In addition, commercial electronic messages shall satisfy the following criteria:

- commercial electronic messages shall unequivocally be identified as such;
- the recipient shall have easy access to information regarding the person sending the message as stipulated by the Law of Ukraine "On Electronic Commerce", in particular: (i) full name of legal entity/individual; place of registration/residence; (ii) email/web-site of online shop; (iii) registration number or tax ID number/passport details (for individuals); (iv) licence data (in case if it is mandatory under the law); (v) inclusion of taxes in calculation of the price of goods/services; and (vi) price of delivery of goods (in case if delivery is performed)); and

- commercial electronic messages regarding sales, promotional gifts, premiums etc. shall be unequivocally identified as such and conditions of receiving of such promotions shall be clearly stated to avoid their ambiguous understanding as well as shall comply with advertising legislation.

When electronic marketing involves the processing of an individual's personal data, it should take place in compliance with the requirements of Ukrainian data protection legislation.

Considering the requirements of the Data Protection Law outlined above, in order for the use of an individual's personal data for electronic marketing purposes, there is a requirment to obtain appropriate consent from the individual which would allow for the processing of his / her personal data for such purposes.

ONLINE PRIVACY

There is no specific legislation regulating the sphere of online privacy in Ukraine. However, the Data Protection Law applies to the extent online activities involve the processing of personal data.

KEY CONTACTS

Natalia Pakhomovska
Partner
T +380 44 495 1789
natalia.pakhomovska@dlapiper.com

Natalia Kirichenko
Senior Associate
T +380 44 490 9575
natalia.kirichenko@dlapiper.com

Roman Inozemtsev
Associate
T +380 44 490 9575
roman.inozemtsev@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

UNITED KINGDOM

Last modified 19 October 2015

LAW IN UNITED KINGDOM

As a member of the European Union, the United Kingdom implemented the EU Data Protection Directive 95/46/EC in March 2000 with the Data Protection Act 1998 ('Act'). Enforcement is through the Information Commissioner's Office ('ICO').

DEFINITIONS

Definition of personal data

'Personal data' is defined under the Act as data relating to living individuals who can be identified:

- from the data, or
- from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Definition of sensitive personal data

'Sensitive personal data' means personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

T +0303 123 1113 (or +44 1625 545745 if calling from overseas)
F 01625 524510

www.ico.org.uk

REGISTRATION

Data controllers who process personal data must inform the Information Commissioner so that their processing of personal data may be registered and made public in the register of data controllers, unless an exemption applies.

The registration is made via a simple online form and the ICO allows data controllers to use standard form sector specific descriptions of their processing when registering. These description set out in very broad terms

- what data is being collected
- why the data will be processed
- the categories of data subject data is collected from, and
- whether the data will be transferred either within or outside the European Economic Area.

However, data controllers can also provide their own specific description of the their processing or tailor the standard form sector specific descriptions if they wish.

DATA PROTECTION OFFICERS

There is no requirement in the UK for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject consents
- the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party
- the processing satisfies the data controller's legal obligation
- the processing protects the data controller's vital interests
- the processing is required by an enactment, the Crown or the government
- the processing is required to perform a public function in the public interest, or to administer justice, or
- the data controller has a legitimate reason for the processing, except if the processing would damage the data subject's rights, freedoms or other legitimate interests.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions.

Whichever of the above conditions is relied upon, the data controller must provide the data subject with fair processing information. This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

Data controllers may transfer personal data out of the European Economic Area if any of the following conditions are met:

- the data subject consents.
- the transfer is essential to a contract to which the data subject is party.
- the transfer is needed to carry out a contract between the data controller and a third party if the contract serves the data subject's interests.
- the transfer is legally required or essential to an important public interest.
- the transfer protects the data subject's vital interests, or
- the data is public.

Transfers of personal data to jurisdictions outside of the European Economic Area are allowed if the jurisdiction provides 'adequate protection' for the security of the data, or if the transfer is covered by 'standard contractual clauses' approved by the European Commission, or subject to an organisation's Binding Corporate Rules. There is no requirement in the UK to notify the ICO of the use of the standard contractual clauses or to file these with the ICO.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles can satisfy the requirements of the UK's transfer restrictions.*

**** Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.***

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data.

The Act does not specify specific security measures to adopt and implement. However, the ICO recommends that organisations should adopt best practice methodologies such as ISO 27001.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the ICO or to data subjects. However, ICO guidance indicates that if a large number of people are affected or the consequences of the breach are particularly serious, the ICO should be informed.

Sector specific regulations/guidance do impose obligations to notify the relevant regulator and data subjects in the event of a security breach (eg the Financial Conduct Authority).

Mandatory breach notification

None contained in the Act. However, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PEC Regulations'), as amended, require providers of a public electronic communications service to notify the ICO (and in some cases subscribers) in the event of a personal data breach.

Failure to notify can result in a fine of GBP 1,000 and negative publicity.

ENFORCEMENT

In the UK the ICO is responsible for the enforcement of the Act. If the ICO becomes aware that a data controller is in breach of the Act, he can serve an enforcement notice requiring the data controller to rectify the position. Failure to comply with an enforcement notice is a criminal offence and can be punished with fines of up to GBP 5,000 in the Magistrates' Court or with unlimited fines in the Crown Court.

The ICO can impose fines of up to GBP 500,000 for serious breaches of the Act. This penalty, introduced in April 2010, can be imposed in respect of breaches of the data protection principles which are:

- serious, and
- likely to cause substantial damage or distress and either
    - the contravention was deliberate, or
    - the data controller knew or ought to have known that there was a risk that the breach would occur and would be likely to cause substantial damage or distress, but failed to take reasonable steps to prevent the breach.

Financial services firms regulated by the Financial Conduct Authority (FCA) may find that a breach of the Act may also give rise to enforcement action by the FCA in respect of a breach of the FCA Principles for Business. The FCA enforcement powers are extensive and can include unlimited fines.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (eg a right to 'opt-out') for direct marketing purposes.

There are a number of different opt-out schemes/preference registers for different media types. Individuals (and, in some cases, corporate subscribers) can contact these schemes and ask to be registered as not wishing to receive direct marketing material. If advertising materials are sent to a person on the list, sanctions can be levied by the ICO using his powers under the Act.

The PEC Regulations prohibit the use of automated calling systems without the consent of the recipient. The PEC Regulations also prohibit unsolicited electronic communications (ie by email or SMS text) for direct marketing purposes without prior consent from the consumer unless:

- the consumer has provided their relevant contact details in the course of purchasing a product or service from the person proposing to undertake the marketing
- the marketing relates to offering a similar product or service, and
- the consumer was given a means to readily 'opt out' of use for direct marketing purposes both at the original point where their details were collected and in each subsequent marketing communication.

Each direct marketing communication must not disguise or conceal the identity of the sender and include the 'unsubscribe' feature referred to above.

The restrictions on marketing by email / SMS only applies in relation to individuals and not where marketing to corporate subscribers.

ONLINE PRIVACY

The PEC Regulations (as amended) deal with the collection of location and traffic data by public electronic communications services providers ('CSPs') and use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication.

However, Traffic Data can be retained if:

- it is being used to provide a value added service, and
- consent has been given for the retention of the Traffic Data.

Traffic Data can also be processed by a CSP to the extent necessary for:

- the management of billing or traffic
- dealing with customer enquiries
- the prevention of fraud, or
- the provision of a value added service.

Cookie Compliance

The use and storage of cookies and similar technologies requires:

- clear and comprehensive information, and
- consent of the website user.

The ICO has confirmed that consent can be implied where a user proceeds to use a site after being provided with clear notice (eg by way of a pop-up or banner) that use of site will involve installation of a cookie.

Consent is not required for cookies that are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the PEC Regulations is dealt with by the ICO and sanctions for breach are the same as set out in the enforcement section above.

KEY CONTACTS

Andrew Dyson
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +44 (0)113 369 2403
andrew.dyson@dlapiper.com

Ross McKean
Partner&Co-Chair of EMEA Data Protection and Privacy Group
T +44 (0) 20 7796 6077
ross.mckean@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

UNITED STATES

Last modified 27 January 2016

LAW IN UNITED STATES

The United States has about 20 sector specific or medium-specific national privacy or data security laws, and hundreds of such laws among its 50 states and its territories. (California alone has more than 25 state privacy and data security laws). These laws, which address particular issues or industries, are too diverse to summarize fully in this volume.

In addition, the large range of companies regulated by the Federal Trade Commission ('FTC') are subject to enforcement if they engage in materially unfair or deceptive trade practices. The FTC has used this authority to pursue companies that fail to implement reasonable minimal data security measures, fail to live up to promises in privacy policies, or frustrate consumer choices about processing or disclosure of personal data.

DEFINITIONS

Definition of personal data

Varies widely by regulation. The FTC now considers information that can reasonably be used to contact or distinguish a person, including IP addresses and device identifiers, as personal data. However, very few U.S. federal or state privacy laws define "personal information" as including information that on its own does not actually identify a person.

Definition of sensitive personal data

Varies widely by sector and by type of statute. Generally personal health data, financial data, credit worthiness data, student data, personal information collected online from children under 13, and information that can be used to carry out identity theft or fraud are considered sensitive. For example, US state data security breach notice and state data security laws typically cover name plus government identification number, financial account or payment card number, and in some states health insurance medical and/or biometric data, and user name and password for an online account.

NATIONAL DATA PROTECTION AUTHORITY

No official national authority. However, the FTC has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (eg for telemarketing, commercial email, and children's privacy). The FTC uses its general authority to prevent unfair and deceptive trade practices to bring enforcement actions against inadequate data security measures, and inadequately disclosed information collection, use and disclosure practices. State attorneys general typically have similar authority and bring some enforcement actions, particularly in the case of high profile data security breaches.

In addition, a wide range of sector regulators, particularly those in the health care, financial services, communications, and insurance sectors, have authority to issue and enforce privacy regulations.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

With the exception of entities regulated by HIPAA, there is no requirement to appoint a data protection officer, although appointment of a chief privacy officer and an IT security officer is a best practice among larger organisations and increasingly among mid sized ones. In addition, Massachusetts law requires an organization to appoint one or more employees to maintain its information security program. The law applies to organizations that own or license personal data on residents of Massachusetts, and thus reaches outside the state.

COLLECTION & PROCESSING

US privacy laws and self regulatory principles vary widely, but generally require pre collection notice and an opt out for use and disclosure of regulated personal information.

Optin rules apply in special cases involving information that is considered sensitive under US law, such as for health information, use of credit reports, student data, personal information collected online from children under 13 (see below for the scope of this requirement), video viewing choices, precise geolocation data, and telecommunication usage information. The FTC interprets as a "deceptive trade practice" failing to obtain opt in consent if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was collected. It has, for example, sued to prevent disclosure of personal data as aprt of serveral bankruptcy proceedings.

States impose a wide range of specific requirements, particularly in the employee privacy area. For example, a significant number of states have enacted employee social media privacy laws, and, in 2014 and 2015, a disparate array of education privacy laws.

The US also regulates marketing communications extensively, including telemarketing, text message marketing, fax marketing and email marketing (which is discussed below). The first three types of marketing are frequent targets of class action lawsuits for significant statutory damages.

TRANSFER

No geographic transfer restrictions apply in the US, except with regard to storing some government information. The

Commerce Clause of the U.S. Constitution likely bars US states from imposing data transfer restrictions and there are no other such restrictions in US national laws.

Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C362/14) the USEU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US.

SECURITY

Most US businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (eg health or financial information, telecommunications usage information, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for data elements that trigger security breach notice requirements. For example, Massachusetts has enacted regulations which apply to any company that collects or maintains sensitive personal information (eg name

in combination with Social Security number, driver's license, passport number, or credit card or financial account number) on Massachusetts residents. Among other things, the Massachusetts regulations require regulated entities to have a comprehensive, written information security program; the regulations also set forth the minimum components of such program, including binding all service providers who touch this sensitive personal information data to protect it in accordance with the regulations. Both Nevada and Massachusetts laws impose encryption requirements on the transmission of sensitive personal information across wireless networks or beyond the logical or physical controls of an organization, as well as on sensitive personal data stored on laptops and portable storage devices.

HIPAA regulated entities are subject to much more extensive data security requirements, and some states impose further security requirements (eg for payment card data, for social security numbers, or to employ secure data destruction methods). HIPAA security regulations apply to so-called 'covered entities' such as doctors, hospitals, insurers, pharmacies and other health-care providers, as well as their 'business associates' which include service providers who have access to, process, store or maintain any protected health information on behalf of a covered entity. 'Protected health information' under HIPAA generally includes any personally identifiable information collected by or on behalf of the covered entity during the course of providing its services to individuals.

Federal financial regulators impose extensive security requirements on the financial services sector, including requirements for security audits of all service providers who receive data from financial institutions.

BREACH NOTIFICATION

Security breach notification requirements are a US invention. 47 US states, Washington, D.C. and most US territories (including, Puerto Rico, Guam and the Virgin Islands) require notifying state residents of a security breach involving residents" name plus a sensitive data element typically, social security number, other government ID number, or credit card or financial account number. In a growing minority of states, sensitive data elements also include medical information, health insurance numbers, biometric data, and login credentials (ie username and password). Also, date of birth, tax ID, shared security "secrets", and birth and marriage certificates are each considered sensitive data under the breach notice laws of at least one state.

Notice of larger breaches is typically required to be provided to credit bureaus, and in minority of states, to State Attorneys Generals and/or other state officials. Federal laws require notification in the case of breaches of health care information, breaches of information from financial institutions, breaches of telecomm usage information held by telecomm services, and breaches of government agency information.

ENFORCEMENT

Violations are generally enforced by the FTC, State Attorneys General, or the regulator for the industry sector in question. Civil penalties are generally significant. In addition, some privacy laws (for example, credit reporting privacy laws, electronic communications privacy laws, video privacy laws, call recording laws, cable communications privacy laws) are enforced through class action lawsuits for significant statutory damages and attorney's fees. Defendants can also be sued for actual damages for negligence in securing personal information such as payment card data, and for surprising and inadequately disclosed tracking of consumers.

ELECTRONIC MARKETING

The US regulates marketing communications extensively, including email and text message marketing, as well as telemarketing and fax marketing.

E-mail

The CAN-SPAM Act is a federal law that applies labelling and opt-out requirements to all commercial email messages. CAN-SPAM generally allows a company to send commercial emails to any recipient, provided the recipient has not opted out of receiving such emails from the sender, the email identifies the sender and the sender's contact information,

and the email contains instructions on how the recipient can easily and without cost opt out of future commercial emails from the sender. Not only the FTC and State Attorneys General, but also ISPs and corporate email systems can sue violators. Furthermore, knowingly falsifying the origin or routing of a commercial email message is a federal crime.

Text Messages

Federal and state regulations apply to the sending of marketing text messages to individuals. Express consent is required to send text messages to individuals, and, for marketing text messages, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any text messaging (marketing or informational) needs to be carefully reviewed for strict compliance with legal requirements.

Telemarketing

In general, federal law applies to most telemarketing calls and programs, and a state's telemarketing law will apply to telemarketing calls placed to or from within that particular state. As a result, most telemarketing calls are governed by federal law, as well as the law of one or more states. Telemarketing rules vary by state, and address many different aspects of telemarketing. For example, national ('federal') and state rules address calling time restrictions, honouring do-not-call registries and opt-out requests, mandatory disclosures to be made during the call, requirements for completing a sale, executing a contract or collecting payment during the call, restrictions on the use of auto-dialers and pre-recorded messages, and record keeping requirements. Many states also require telemarketers to register or obtain a license to place telemarketing calls.

Callers generally must scrub their calling lists against both a national and multiple state do-not-call registries, as it is prohibited to place a telemarketing call to a number listed in a do-not call registry unless a specific exemption applies. The national do-not-call rules (and several state rules), for example, exempt calls to existing business customers who have purchased a product or service in the last 18 months from the company on whose behalf the call is placed, as long as the customer has not specifically opted out of receiving telemarketing calls from the company. The use of auto-dialers to send pre-recorded messages generally requires affirmative opt-in consent of the recipient.

Fax Marketing

Federal law and regulations generally prohibit the sending of unsolicited advertising by fax without prior, express consent. Violations of the law are subject to civil actions and have been the subject of numerous class action lawsuits. The law exempts faxes to recipients that have an established business relationship with the company on whose behalf the fax is sent, as long as the recipient hasn't opted out of receiving fax advertisements and has provided their fax number 'voluntarily,' a concept which the law specifically defines. The law also requires that each fax advertisement contain specific information, including (i) a 'clear and conspicuous' opt out method on the first page of the fax; (ii) a statement that the recipient may make a request to the sender not to send any future faxes and that failure to comply with the request within 30 days is unlawful; and (iii) a telephone number, fax number, and cost-free mechanism to opt-out of faxes, which permit consumers to make opt-out requests 24 hours a day, seven days a week.

ONLINE PRIVACY

Online Privacy Policy Requirement

The States of California and Delaware require commercial online websites and mobile applications to post a relatively general online privacy policy. Liability for failing to post the privacy policy may only be imposed if the website or mobile app is notified of its non-compliance and fails to post the policy with 30 days of receiving notice of non-compliance.

Cookies

There is no specific federal law that regulates the use of cookies, web beacons, Flash LSOs and other similar tracking mechanisms. However, the Children's Online Privacy Protection Act (COPPA) applies to information collected automatically (eg via cookies) from child-directed websites and other websites and third party ad networks or plug-ins

that knowingly collect personal information online from children under 13, COPPA also regulates behavioural advertising to children under 13.

In addition, undisclosed online tracking of customer activities poses class action risk. The use of cookies and similar tracking mechanisms should be carefully and fully disclosed in a website privacy policy. Furthermore, it is a best practice for websites that allow behavioural advertising on their websites to participate in the Digital Advertising Alliance code of conduct, which includes displaying an icon from which users can opt out of being tracked for behavioural advertising purposes. Under California law, any company that tracks any personally identifiable information about consumers over time and across multiple websites must disclose in its privacy policy whether the company honours any 'Do-Not-Track' method or provides users a way to opt out of such tracking; however, the law does not mandate that companies provide consumers a 'Do-Not-Track' option. The same law also requires website operators to disclose in their privacy policy whether any third parties may collect any personally identifiable information about consumers on their website and across other third party websites, and prohibits the advertsing of certain products, services and materials (including alcohol, tobacco, firearms, certain dietarty supplements, ultraviolet tanning, tattoos, obscene matters, etc).

Minors

California law requires that operators of websites or online services that are directed to minors or that knowingly collect personally identifiable information from minors permit minors that are registered users of their sites to remove any content the minor has posted from the site or online service. The law does not give minors the right to remove information posted by third parties. Minors must be given clear notice on how to exercise their right to removal.

Location Data

Privacy requirements of location based apps and services is in flux and is a subject of extensive interest and debate. Federal Communications Commission regulations govern the collection and disclosure of location information by telecommunications carriers, including wireless carriers. Further, any location service that targets children under the age of 13 or has actual knowledge that it is collecting location information from children under age 13 must comply with the requirements of the COPPA Rules including obtaining prior verifiable parental consent in most circumstances. Both the Federal Trade Commission and California Attorney General's Office have issued best practices recommendations for mobile apps and mobile app platforms, and the California Attorney General has entered into an agreement with major app platforms in which they promise to prompt mobile apps to post privacy policies. Furthermore, a Department of Commerce led multi stakeholder negotiation to develop a code of conduct for mobile app privacy is well underway.

KEY CONTACTS

Jim Halpert
Partner & Chair of US Data Protection and Privacy Group
T +1 202 799 4441
jim.halpert@dlapiper.com

Jennifer Kashatus
Partner, Data Protection, Privacy and Security
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

Kate Lucente
Associate and Co-Editor, Data Protection Laws of World Handbook
T +1 813 222 5927
kate.lucente@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

URUGUAY

Last modified 28 January 2015

LAW IN URUGUAY

Data Protection Act Law No. 18.331 (11 August 2008); Decree No. 414/009 (31 August 2009) (the 'Act').

DEFINITIONS

Definition of personal data

Any kind of information related to an identified or identifiable person or legal entity.

Definition of sensitive personal data

Any kind of personal data evidencing: racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership as well as any kind of information concerning health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

('URCDP', *Unidad Reguladora y de Control de Datos Personales* ('Data Protection Authority').

REGISTRATION

Every database must be registered with the Data Protection Authority in Uruguay if the information contained in the database is gathered or obtained through means, mechanisms or sources located in Uruguay.

The database must be registered by filing mandatory forms, which must be signed by a representative of the company that owns the data base.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

In order to collect personal data contained in a database, the data processor must first obtain prior, documented consent from the individual or entity whose information is being processed. Documented consent is not required in the following cases:

- personal data obtained from public sources
- personal data obtained by public bodies to comply with legal obligations

- personal data limited to domicile address, telephone number, ID number, nationality, tax number, corporation name
- personal data obtained based on a contractual or professional relationship, which is necessary to perform the contract or the development of the professional services to be rendered, or
- personal data obtained by individuals or corporations for their personal and exclusive use.

The personal data processed cannot be used for secondary purposes, which are different from those that have justified the initial acquisition of the information. There must be legitimate reasons (ie, reasons which are not against the law) for the processing of the personal information. The Act further establishes that once the reasons to process the personal information are no longer present, the personal information must be deleted.

TRANSFER

Personal data can only be transferred to a third party:

- for purposes directly related to the legitimate interests of the transferring party and the transferee, and
- with the prior consent of the data subject. However, such consent may be revoked. Additionally, the data subject must be informed of the purpose of the transfer, as well as of the identity of the recipient.

However, the prior consent of the data subject is not necessarily required when the personal data to be transferred is limited to: name, surname, identity card number, nationality, address, and date of birth.

The purpose and proper identification of the transferee must be included in the request for consent addressed to the data subject. Evidence of the data subject's consent must be kept in the files of the data processor.

If the data subject's consent is not obtained within ten business days (counted from the receipt of the communication from the data processor asking for the consent), it will be construed that the data subject did not consent to the transfer of the data.

Upon the transfer, the data processor will remain jointly and severable liable for the compliance of the recipient's obligations under the Act.

The Act forbids the transfer of personal data to countries or international entities which do not provide adequate levels of protection (according to European standards). However, the Act allows international transfer to unsafe countries or entities when the data subject consents to the transfer (such consent must be given in writing), or when the guarantees of adequate protection levels arise from 'contractual clauses', and 'self-regulation systems'.

The international data transfer agreement must provide for the same levels of protection which are effective under the laws of Uruguay.

In the case of a cross border transfer within a group of companies, Uruguayan laws establish that the international transfer will be lawful without any authorisation whenever the recipient branch has adopted a conduct of code duly registered with the local URCDP.

The international transfer of personal data between headquarters and their respective branches or subsidiaries is authorised when the headquarters and their branches have a code of conduct (such as an inter-company agreement) duly filed with URCDP.

SECURITY

Data processors must implement appropriate technical and organisational measures to guarantee the security and confidentiality of the personal data. These measures should be aimed at preventing the loss, falsification, and unauthorised treatment or access, as well as at detecting information that may have been lost, leaked, or accessed

without authorisation.

It is prohibited to register personal data in databases which do not meet technical safety conditions.

BREACH NOTIFICATION

In case the data processor detects a breach of security measures, and if the consequences of the breach could substantially affect the rights of the data subject and/or the rights of any other agent or person involved, the data processor should report the breach to the affected persons.

ENFORCEMENT

The URCDP is responsible for enforcement of the Act. In the context of its powers, the URCDP has broad investigatory powers, including audit and inspection rights, and subpoena, search and seizure authority.

The URCDP has the authority to impose penalties against the data processor in the following order: warning, admonition, fines up to USD 60,000, suspension of the database for five days, closure of the database.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as these activities typically involve the processing and use of personal data (eg an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing, but grants personal data owners/ data subjects (individuals or legal entities) the right to demand the deletion or suppression of their data from the marketing database.

Personal data may be used and processed for marketing purposes when the personal data was either obtained from public documents, provided by the data subject or when prior consent has been gathered.

ONLINE PRIVACY

There are no provisions that specifically address online tracking or geolocation data. However, the general principles of the Act apply. The personal data processed cannot be used for purposes other than those that justified the acquisition of the data; and when the reasons to process the personal information have expired, the personal information must be deleted.

KEY CONTACTS

Estudio Bergstein
www.bergsteinlaw.com/

Jonas Bergstein
Partner
T +598 2 901 2448
jbergstein@bergsteinlaw.com

Guzmán Ramírez
T +598 2901 2448
gramirez@bergsteinlaw.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

VENEZUELA

Last modified 26 January 2015

LAW IN VENEZUELA

Venezuela does not have any general legislation regulating data protection. However, there are general principles established in the Constitution of the Bolivarian Republic of Venezuela (the 'Constitution') and developed by Supreme Court decisions.

The Constitution establishes certain principles which serve as framework for the protection of personal data, because their purpose is to safeguard the honour, private life, intimacy, self-image, confidentiality and reputation of people. The Constitution also establishes the right of access to information and data.

Article 28 of the Constitution guarantees everyone access to the information and data on themselves, stored in public or private registries, and the right to be aware of the uses of such information, as well as the right to update, rectify or destroy incorrect information that unlawfully affects their rights.

The Constitutional Chamber of the Supreme Court of Justice has acknowledged the possibility that a person or entity may collect and maintain information on individuals and their goods/purchases, arranged in such way that a profile of individuals, their activities, or their goods can be made, with the purpose of using them for the benefit of the collecting entity or of third parties, provided that all constitutional rights are respected, and in particular the ones established in Article 28 of the Constitution. Whoever collects and records information on individuals and their goods, must respect the right of every person to protect his honor, private life, intimacy, self-image, confidentiality and reputation, which is granted in Article 60 of the Constitution.

Also, in accordance with a binding decision of the Constitutional Chamber, any person who collects and manages personal information must guarantee the following principles:

- Principle of free will
- Principle of legality
- Principle of purpose and quality
- Principle of temporality or conservation
- Principle of accuracy and self-determination
- Principle of security and confidentiality
- Principle of guardianship
- Principle of responsibility (collectively called the 'Principles').

There are also specific provisions concerning data protection with limited scope of application, contained in the Banking Institutions Law and the Special Law against Cybercrime.

DEFINITIONS

Definition of personal data

There is no legal definition of 'personal data' established in any particular law.

Definition of sensitive personal data

There is no legal definition of 'personal data' established in any particular law.

NATIONAL DATA PROTECTION AUTHORITY

Venezuela does not have a national data protection authority. Some agencies have data protection authority within their specific jurisdiction, for instance, the Superintendence of Banks and the National Telecommunications Commission.

REGISTRATION

There is no legal requirement to register databases.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Based on principles set forth by case law (specifically the principle of free will) and the Constitution, there is a requirement to obtain prior consent to collect, use, and transfer personal data submitted by a data subject. Based on the same principle, consent may be revoked at any time.

Pursuant to the Constitution, everyone must be granted access to information and data on themselves, stored in public or private registries, and every person has the right to be aware of the use of such information, as well as the right to update, rectify or destroy incorrect information that unlawfully affects their rights.

Also, in accordance with a binding decision of the Constitutional Chamber any person who collects and manages personal information must guarantee the following principles:

- Principle of free will
- Principle of legality
- Principle of purpose and quality
- Principle of temporality or conservation
- Principle of accuracy and self-determination
- Principle of security and confidentiality
- Principle of guardianship
- Principle of responsibility (collectively called the 'Principles').

TRANSFER

Transfer of data to third parties would be subject to the provisions set forth by the Constitution and by case law, including confidentiality and security obligations, and appropriate measures should be taken in order to obtain the necessary consents prior to such data being distributed.

SECURITY

Under banking regulations, banking institutions in Venezuela are prohibited from disclosing personal information unless consent is obtained, in writing. Also, data controllers must take reasonable technical and organizational measures to ensure the security of personal data.

BREACH NOTIFICATION

There is no legal requirement to report data security breaches. However, according to the Banking Institutions Law and its regulations, the notification of personal data breaches may be provided by the Superintendence of Banks to affected users or their authorized representatives.

ENFORCEMENT

There is no data protection authority in Venezuela. Enforcement can occur through administrative procedures, criminal procedures, individual civil lawsuits and class actions, which can be initiated by the affected individual or by public authorities. Some agencies have data protection authority within their specific jurisdiction, for instance, the Superintendence of Banks and the National Telecommunications Commission.

ELECTRONIC MARKETING

There is no law that specifically regulates electronic marketing. However, in November 2014, the National Assembly approved, in first reading, the bill on Electronic Commerce. This Law intends to establish security and data protection requirements, protections for online transactions, security of payment information, and restrictions on use of information and data collected in an e-commerce context.

Also, the Law states that any provider of goods or services shall ensure people's privacy and the confidentiality of information involved in transactions, so that information exchanged is not accessible to unauthorized third parties.

ONLINE PRIVACY

There is no law that specifically addresses online privacy or cookies. However, the Special Law against Cybercrime establishes a penalty of imprisonment and fine if any person intentionally uses, amends, alters or discloses by any means, without the consent of the system owner, the data or personal information contained in a computer or in any other technological system.

KEY CONTACTS

DLA Interjuris Abogados, S.C.
www.dlainterjuris.com/

María Cecilia Rachadell
Founding Partner
T +58 (212) 2662613
maria.rachadell@dlainterjuris.com

Gabriella Rachadell
Partner
T +58 (212) 2662613
gabriela.rachadell@dlainterjuris.com

Alessandra Chumaceiro Briceño
Attorney
T +58 (212) 7501200
alessandra.chumaceiro@dlainterjuris.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.

ZIMBABWE

Last modified 25 January 2016

LAW IN ZIMBABWE

The protection of privacy is a principal enshrined in Zimbabwe's Constitution. Whilst there is no designated national legislation dealing with data protection for private persons in Zimbabwe, however there are laws that have a bearing on the right to privacy and protection of personal information for specific types of data, or in relation to specific activities.

The Access to Information and Protection of Privacy Act (Chapter 10:247) is the law which contains the most provisions on data protection. However, this generally only regulates the use of personal data by public bodies.

Other laws refer to the protection of information as a function of other activities or the protection of specific types of data such as the Courts and Adjudicating Authorities (Publicity Restrictions) Act (Chapter 07:04), the Census and Statistics Act (Chapter 10:29), Banking Act (Chapter 24:20), National Registration Act (Chapter 10:17) and the Interception of Communications Act (Chapter 11:20).

The Ministry of Information Communication Technology and Postal Services is currently formulating the policy principles for a data protection law.

DEFINITIONS

Definition of personal data

The Access to Information and Protection of Privacy Act defines personal information as recorded information about an identifiable person which includes:

- the person's name, address or telephone number
- the person's race, national or ethnic origin, religious or political beliefs or associations
- the person's age, sex, sexual orientation, marital status or family status
- an identifying number, symbol or other particulars assigned to that person
- fingerprints, blood type or inheritable characteristics
- information about a person's health care history, including a physical or mental disability
- information about educational, financial, criminal or employment history
- a third party's opinions about the individual
- the individual's personal views or opinions, (except if they are about someone else), and
- personal correspondence with home or family.

Definition of sensitive personal data

There is no law which defines sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

There is no data protection authority. However, the Zimbabwe Media Commission's mandate does include the following:

- ensuring that the people of Zimbabwe have equitable and wide access to information
- commenting on the implications of proposed legislation or programmes of public bodies on access to information and protection of privacy
- commenting on the implications of automated systems for collection, storage, analysis or transfer of information or for the access to information or protection of privacy
- amongst other functions.

REGISTRATION

There is no law that requires the registration of databases.

DATA PROTECTION OFFICERS

There is no provision to appoint data protection officers.

COLLECTION & PROCESSING

There are no specific provisions for the collectors of personal data to obtain the prior approval of data subjects for the processing of their personal data.

The Census and Statistics Act contains provisions which restrict the use and disclosure of information obtained during the conducting of a census exercise. Under this act authorities are authorised to collect, compile, analyse and abstract statistical information relating to the:

- commercial
- industrial
- agricultural
- mining
- social
- economic
- and general activities and conditions of the inhabitants of Zimbabwe and to publish such statistical information.

TRANSFER

The transfer of personal data to any other jurisdiction is not specifically restricted.

SECURITY

There is no law which requires data controllers and processors to implement particular technological measures to ensure the security of information. However, there are laws that require recipients of personal information to guarantee a certain level of security to ensure that personal private data is not improperly disclosed. These laws are only applicable to personal information collected during the course of official duty, such as in court proceedings, a census, banking transactions and national registration processes.

For example, the Banking Act provides for the registration, supervision and regulation of persons conducting banking business and financial activities in Zimbabwe. The provisions of this Act restrict the disclosure and use of collected information by the Registrar of the Reserve Bank, his representatives or employees or a curator or an auditor of the Banking Institution, but do not however deal with the Banking Institutions specifically.

BREACH NOTIFICATION

Breach notification

There is no law which requires data protection officers to report a breach.

Mandatory breach notification

There are no mandatory breach notification provisions.

ENFORCEMENT

The Constitution mandates the Human Rights Commission (HRC) to enforce a citizen's human rights where they have been violated. The right to privacy, including the right not to have the privacy of one's communication infringed is enshrined as a basic human right, which therefore falls within the purview of the HRC. However, the Monitoring of Interception of Communications Centre (MICC), established by the Interception of Communications Act, is mandated to, among other things, monitor communications made over telecommunications, radio communications and postal systems and to give technical advice to service providers. The mandate of the MICC does not preclude it from monitoring computer based data for the purposes of enforcing an individual's right to privacy where it is found that such right has been infringed.

ELECTRONIC MARKETING

The Government is currently working on a Consumer Protection Act, which seeks to protect consumers from unscrupulous traders. The draft Consumer Protection Bill does not make reference to electronic marketing, nor does it provide for consumer privacy rights regarding in respect of personal data.

ONLINE PRIVACY

There is currently no specific online privacy legislation.

KEY CONTACTS

Manokore Attorneys
www.corporatecounsel.co.zw

Bridget Mafusire
Associate
T +263 4 746 787
bmafusire@corporatecounsel.co.zw

Lloyd Manokore
Partner
T +263 4 746 787
lmanokore@corporatecounsel.co.zw

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.